



(translation of the front page of the priority document of
Japanese Patent Application No. 2001-193446)

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the
following application as filed with this Office.

Date of Application: June 26, 2001

Application Number : Patent Application 2001-193446

[ST.10/C] : [JP 2001-193446]

Applicant(s) : Canon Kabushiki Kaisha

February 22, 2002

Commissioner,

Japan Patent Office

Kouzo OIKAWA

Certification Number 2002-3009935

CFM 2495 US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 6月26日

出 願 番 号

Application Number:

特願2001-193446

[ST.10/C]:

[JP2001-193446]

出 願 人

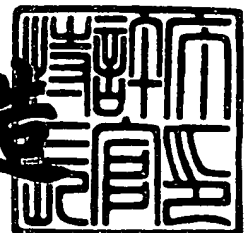
Applicant(s):

キヤノン株式会社

2002年 2月22日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 4353009

【提出日】 平成13年 6月26日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明の名称】 データ保存サービス装置、制御方法、及びシステム、制御プログラム

【請求項の数】 70

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

 【氏名】 浜田 正志

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

 【代表者】 御手洗 富士夫

【代理人】

 【識別番号】 100081880

 【弁理士】

 【氏名又は名称】 渡部 敏彦

 【電話番号】 03(3580)8464

【手数料の表示】

 【予納台帳番号】 007065

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9703713

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ保存サービス装置、制御方法、及びシステム、制御プログラム

【特許請求の範囲】

【請求項 1】 ネットワークを介して保存要求されたデータを保存するための複数のサーバを備えたデータ保存サービス装置において、

少なくともユーザのサービス加入条件のレベルに応じて前記サーバを選択する選択手段と、

前記選択手段により選択されたサーバに対して保存要求に係るデータを格納する格納制御手段と、

を含むサービス制御手段を有することを特徴とするデータ保存サービス装置。

【請求項 2】 前記選択手段は、少なくとも 2 つ以上の前記サーバを選択することを特徴とする請求項 1 記載のデータ保存サービス装置。

【請求項 3】 前記格納制御手段は、前記選択手段により選択されたサーバに対応する暗号化方式で保存要求に係るデータを暗号化して当該選択に係るサーバに格納することを特徴とする請求項 1 又は 2 記載のデータ保存サービス装置。

【請求項 4】 前記サービス加入条件のレベルは、契約料金等のサービスに対する対価に基づいて決定されていることを特徴とする請求項 1 ～ 3 の何れかに記載のデータ保存サービス装置。

【請求項 5】 前記サービス加入条件のレベルは、契約継続年数等のサービスの享受期間に基づいて決定されていることを特徴とする請求項 1 ～ 4 の何れかに記載のデータ保存サービス装置。

【請求項 6】 前記選択手段は、災害情報に基づいて前記サーバを選択することを特徴とする請求項 1 ～ 5 の何れかに記載のデータ保存サービス装置。

【請求項 7】 前記選択手段は、保存要求を行ったクライアント機器の存在地域を考慮して前記サーバを選択することを特徴とする請求項 1 ～ 6 の何れかに記載のデータ保存サービス装置。

【請求項 8】 前記選択手段は、保存要求を行ったユーザのサービス加入条件のレベルに対応する前記サーバの中から、罹災リスクの最も低いサーバと、

保存要求を行ったクライアント機器の存在地域以外の地域に存在するサーバの中で罹災リスクの最も低いサーバとを選択することを特徴とする請求項 1～7 の何れかに記載のデータ保存サービス装置。

【請求項 9】 前記選択手段は、前記ユーザのサービス加入条件のレベルが変更された場合は前記サーバを選択し直し、前記格納制御手段は、当該選択手段により選択し直されたサーバに対して前記保存要求に係るデータを格納し直すことを特徴とする請求項 1～8 の何れかに記載のデータ保存サービス装置。

【請求項 10】 前記選択手段は、前記災害情報の変化に応じて前記サーバを選択し直し、前記格納制御手段は、当該選択手段により選択し直されたサーバに対して前記保存要求に係るデータを格納し直すことを特徴とする請求項 1～9 の何れかに記載のデータ保存サービス装置。

【請求項 11】 前記選択手段は、前記保存要求を行ったクライアント機器の存在地域が変更された場合は前記サーバを選択し直し、前記格納制御手段は、当該選択手段により選択し直されたサーバに対して当該保存要求に係るデータを格納し直すことを特徴とする請求項 1～10 の何れかに記載のデータ保存サービス装置。

【請求項 12】 前記サービス制御手段は、前記格納制御手段により前記サーバに格納されたデータの正当性を調査する調査手段を含むことを特徴とする請求項 1～11 の何れかに記載のデータ保存サービス装置。

【請求項 13】 前記調査手段は、前記格納制御手段により複数のサーバに格納された保存要求に係る同一のデータ同士を比較することにより、正当性を調査することを特徴とする請求項 12 記載のデータ保存サービス装置。

【請求項 14】 前記調査手段は、メモリ媒体に起因してデータが不当になったのか否かを判別することを特徴とする請求項 12 又は 13 記載のデータ保存サービス装置。

【請求項 15】 前記調査手段は、データの改竄によりデータが不当になったのか否かを判別することを請求項 12～14 の何れかに記載のデータ保存サービス装置。

【請求項 16】 前記調査手段は、データの改竄によりデータが不当になっ

たものと判別した場合、その旨を当該データの保存要求を行ったクライアント機器に通知することを特徴とする請求項 1 5 記載のデータ保存サービス装置。

【請求項 1 7】 前記サービス制御手段は、前記保存要求を行ったユーザが当該サービスの会員であるか否かを認証する認証手段を含み、当該認証手段により認証されたユーザからの保存要求だけを受理することを特徴とする請求項 1 ～ 1 6 の何れかに記載のデータ保存サービス装置。

【請求項 1 8】 前記サービス制御手段は、前記選択手段により選択されたサーバの正当性を認証する認証手段を含み、前記格納制御手段は、当該認証手段により認証されたサーバに対してだけ保存要求に係るデータを格納することを特徴とする請求項 1 ～ 1 7 の何れかに記載のデータ保存サービス装置。

【請求項 1 9】 前記サービス制御手段は、少なくとも前記格納制御手段によるデータ格納処理に関する各種の格納条件データを当該保存要求を行ったクライアント機器に通知する通知手段を含むことを特徴とする請求項 1 ～ 1 8 の何れかに記載のデータ保存サービス装置。

【請求項 2 0】 前記通知手段は、前記格納条件データとして、前記保存要求に係るデータの格納位置データの他に、暗号化のアルゴリズム、暗号鍵のデータを通知することを特徴とする請求項 1 9 記載のデータ保存サービス装置。

【請求項 2 1】 前記クライアント機器は、少なくとも前記通知手段により通知された格納条件データを記憶する記憶手段を有することを特徴とする請求項 1 9 又は 2 0 記載のデータ保存サービス装置。

【請求項 2 2】 前記記憶手段は、前記クライアント機器に着脱可能な記憶媒体であることを特徴とする請求項 2 1 記載のデータ保存サービス装置。

【請求項 2 3】 前記記憶手段は、前記クライアント機器に内蔵された記憶媒体であることを特徴とする請求項 2 1 記載のデータ保存サービス装置。

【請求項 2 4】 ネットワークを介して保存要求されたデータを保存するための複数のサーバを備えたデータ保存サービス装置の制御方法において、少なくともユーザのサービス加入条件のレベルに応じて前記サーバを選択する選択工程と、

前記選択工程により選択されたサーバに対して保存要求に係るデータを格納す

る格納制御工程と、

を含むサービス制御工程を有することを特徴とするデータ保存サービス制御方法。

【請求項 2 5】 前記選択工程は、少なくとも 2 つ以上の前記サーバを選択することを特徴とする請求項 2 4 記載のデータ保存サービス制御方法。

【請求項 2 6】 前記格納制御工程は、前記選択工程により選択されたサーバに対応する暗号化方式で保存要求に係るデータを暗号化して当該選択に係るサーバに格納することを特徴とする請求項 2 4 又は 2 5 記載のデータ保存サービス制御方法。

【請求項 2 7】 前記サービス加入条件のレベルは、契約料金等のサービスに対する対価に基づいて決定されていることを特徴とする請求項 2 4 ～ 2 6 の何れかに記載のデータ保存サービス制御方法。

【請求項 2 8】 前記サービス加入条件のレベルは、契約継続年数等のサービスの享受期間に基づいて決定されていることを特徴とする請求項 2 4 ～ 2 7 の何れかに記載のデータ保存サービス制御方法。

【請求項 2 9】 前記選択工程は、災害情報に基づいて前記サーバを選択することを特徴とする請求項 2 4 ～ 2 8 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 0】 前記選択工程は、保存要求を行ったクライアント機器の存在地域を考慮して前記サーバを選択することを特徴とする請求項 2 4 ～ 2 9 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 1】 前記選択工程は、保存要求を行ったユーザのサービス加入条件のレベルに対応する前記サーバの中から、罹災リスクの最も低いサーバと、保存要求を行ったクライアント機器の存在地域以外の地域に存在するサーバの中で罹災リスクの最も低いサーバとを選択することを特徴とする請求項 2 4 ～ 3 0 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 2】 前記選択工程は、前記ユーザのサービス加入条件のレベルが変更された場合は前記サーバを選択し直し、前記格納制御工程は、当該選択工程により選択し直されたサーバに対して前記保存要求に係るデータを格納し直す

ことを特徴とする請求項 2 4 ～ 3 1 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 3】 前記選択工程は、前記災害情報の変化に応じて前記サーバを選択し直し、前記格納制御工程は、当該選択工程により選択し直されたサーバに対して前記保存要求に係るデータを格納し直すことを特徴とする請求項 2 4 ～ 3 2 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 4】 前記選択工程は、前記保存要求を行ったクライアント機器の存在地域が変更された場合は前記サーバを選択し直し、前記格納制御工程は、当該選択工程により選択し直されたサーバに対して当該保存要求に係るデータを格納し直すことを特徴とする請求項 2 4 ～ 3 4 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 5】 前記サービス制御工程は、前記格納制御工程により前記サーバに格納されたデータの正当性を調査する調査工程を含むことを特徴とする請求項 2 4 ～ 3 4 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 6】 前記調査工程は、前記格納制御工程により複数のサーバに格納された保存要求に係る同一のデータ同士を比較することにより、正当性を調査することを特徴とする請求項 3 5 記載のデータ保存サービス制御方法。

【請求項 3 7】 前記調査工程は、メモリ媒体に起因してデータが不当になったのか否かを判別することを特徴とする請求項 3 5 又は 3 6 記載のデータ保存サービス制御方法。

【請求項 3 8】 前記調査工程は、データの改竄によりデータが不当になったのか否かを判別することを請求項 3 5 ～ 3 7 の何れかに記載のデータ保存サービス制御方法。

【請求項 3 9】 前記調査工程は、データの改竄によりデータが不当になったものと判別した場合、その旨を当該データの保存要求を行ったクライアント機器に通知することを特徴とする請求項 3 8 記載のデータ保存サービス制御方法。

【請求項 4 0】 前記サービス制御工程は、前記保存要求を行ったユーザが当該サービスの会員であるか否かを認証する認証工程を含み、当該認証工程により認証されたユーザからの保存要求だけを受理することを特徴とする請求項 2 4

～ 3 9 の何れかに記載のデータ保存サービス制御方法。

【請求項 4 1】 前記サービス制御工程は、前記選択工程により選択されたサーバの正当性を認証する認証工程を含み、前記格納制御工程は、当該認証工程により認証されたサーバに対してだけ保存要求に係るデータを格納することを特徴とする請求項 2 4 ～ 4 0 の何れかに記載のデータ保存サービス制御方法。

【請求項 4 2】 前記サービス制御工程は、少なくとも前記格納制御工程によるデータ格納処理に関する各種の格納条件データを当該保存要求を行ったクライアント機器に通知する通知工程を含むことを特徴とする請求項 2 4 ～ 4 1 の何れかに記載のデータ保存サービス制御方法。

【請求項 4 3】 前記通知工程は、前記格納条件データとして、前記保存要求に係るデータの格納位置データの他に、暗号化のアルゴリズム、暗号鍵のデータを通知することを特徴とする請求項 4 2 記載のデータ保存サービス制御方法。

【請求項 4 4】 前記クライアント機器は、少なくとも前記通知工程により通知された格納条件データを記憶する記憶手段を有することを特徴とする請求項 4 2 又は 4 3 記載のデータ保存サービス制御方法。

【請求項 4 5】 前記記憶手段は、前記クライアント機器に着脱可能な記憶媒体であることを特徴とする請求項 4 4 記載のデータ保存サービス制御方法。

【請求項 4 6】 前記記憶手段は、前記クライアント機器に内蔵された記憶媒体であることを特徴とする請求項 4 4 記載のデータ保存サービス制御方法。

【請求項 4 7】 ネットワークを介して保存要求されたデータを保存するための複数のサーバを備えたデータ保存サービスシステムにおいて、

少なくともユーザのサービス加入条件のレベルに応じて前記サーバを選択する選択手段と、

前記選択手段により選択されたサーバに対して保存要求に係るデータを格納する格納制御手段と、

を含むサービス制御手段を有することを特徴とするデータ保存サービスシステム。

【請求項 4 8】 前記選択手段は、少なくとも 2 つ以上の前記サーバを選択することを特徴とする請求項 4 7 記載のデータ保存サービスシステム。

【請求項 4 9】 前記格納制御手段は、前記選択手段により選択されたサーバに対応する暗号化方式で保存要求に係るデータを暗号化して当該選択に係るサーバに格納することを特徴とする請求項 4 7 又は 4 8 記載のデータ保存サービスシステム。

【請求項 5 0】 前記サービス加入条件のレベルは、契約料金等のサービスに対する対価に基づいて決定されていることを特徴とする請求項 4 7 ～ 4 9 の何れかに記載のデータ保存サービスシステム。

【請求項 5 1】 前記サービス加入条件のレベルは、契約継続年数等のサービスの享受期間に基づいて決定されていることを特徴とする請求項 4 7 ～ 5 0 の何れかに記載のデータ保存サービスシステム。

【請求項 5 2】 前記選択手段は、災害情報に基づいて前記サーバを選択することを特徴とする請求項 4 7 ～ 5 1 の何れかに記載のデータ保存サービスシステム。

【請求項 5 3】 前記選択手段は、保存要求を行ったクライアント機器の存在地域を考慮して前記サーバを選択することを特徴とする請求項 4 7 ～ 5 2 の何れかに記載のデータ保存サービスシステム。

【請求項 5 4】 前記選択手段は、保存要求を行ったユーザのサービス加入条件のレベルに対応する前記サーバの中から、罹災リスクの最も低いサーバと、保存要求を行ったクライアント機器の存在地域以外の地域に存在するサーバの中で罹災リスクの最も低いサーバとを選択することを特徴とする請求項 4 7 ～ 5 3 の何れかに記載のデータ保存サービスシステム。

【請求項 5 5】 前記選択手段は、前記ユーザのサービス加入条件のレベルが変更された場合は前記サーバを選択し直し、前記格納制御手段は、当該選択手段により選択し直されたサーバに対して前記保存要求に係るデータを格納し直すことを特徴とする請求項 4 7 ～ 5 4 の何れかに記載のデータ保存サービスシステム。

【請求項 5 6】 前記選択手段は、前記災害情報の変化に応じて前記サーバを選択し直し、前記格納制御手段は、当該選択手段により選択し直されたサーバに対して前記保存要求に係るデータを格納し直すことを特徴とする請求項 4 7 ～

55の何れかに記載のデータ保存サービスシステム。

【請求項57】 前記選択手段は、前記保存要求を行ったクライアント機器の存在地域が変更された場合は前記サーバを選択し直し、前記格納制御手段は、当該選択手段により選択し直されたサーバに対して当該保存要求に係るデータを格納し直すことを特徴とする請求項47～56の何れかに記載のデータ保存サービスシステム。

【請求項58】 前記サービス制御手段は、前記格納制御手段により前記サーバに格納されたデータの正当性を調査する調査手段を含むことを特徴とする請求項47～57の何れかに記載のデータ保存サービスシステム。

【請求項59】 前記調査手段は、前記格納制御手段により複数のサーバに格納された保存要求に係る同一のデータ同士を比較することにより、正当性を調査することを特徴とする請求項58記載のデータ保存サービスシステム。

【請求項60】 前記調査手段は、メモリ媒体に起因してデータが不当になったのか否かを判別することを特徴とする請求項58又は59記載のデータ保存サービスシステム。

【請求項61】 前記調査手段は、データの改竄によりデータが不当になったのか否かを判別することを請求項58～60の何れかに記載のデータ保存サービスシステム。

【請求項62】 前記調査手段は、データの改竄によりデータが不当になったものと判別した場合、その旨を当該データの保存要求を行ったクライアント機器に通知することを特徴とする請求項61記載のデータ保存サービスシステム。

【請求項63】 前記サービス制御手段は、前記保存要求を行ったユーザが当該サービスの会員であるか否かを認証する認証手段を含み、当該認証手段により認証されたユーザからの保存要求だけを受理することを特徴とする請求項47～62の何れかに記載のデータ保存サービスシステム。

【請求項64】 前記サービス制御手段は、前記選択手段により選択されたサーバの正当性を認証する認証手段を含み、前記格納制御手段は、当該認証手段により認証されたサーバに対してだけ保存要求に係るデータを格納することを特徴とする請求項47～63の何れかに記載のデータ保存サービスシステム。

【請求項 6 5】 前記サービス制御手段は、少なくとも前記格納制御手段によるデータ格納処理に関する各種の格納条件データを当該保存要求を行ったクライアント機器に通知する通知手段を含むことを特徴とする請求項 4 7 ～ 6 4 の何れかに記載のデータ保存サービスシステム。

【請求項 6 6】 前記通知手段は、前記格納条件データとして、前記保存要求に係るデータの格納位置データの他に、暗号化のアルゴリズム、暗号鍵のデータを通知することを特徴とする請求項 6 5 記載のデータ保存サービスシステム。

【請求項 6 7】 前記クライアント機器は、少なくとも前記通知手段により通知された格納条件データを記憶する記憶手段を有することを特徴とする請求項 6 5 又は 6 6 記載のデータ保存サービスシステム。

【請求項 6 8】 前記記憶手段は、前記クライアント機器に着脱可能な記憶媒体であることを特徴とする請求項 6 7 記載のデータ保存サービスシステム。

【請求項 6 9】 前記記憶手段は、前記クライアント機器に内蔵された記憶媒体であることを特徴とする請求項 6 7 記載のデータ保存サービスシステム。

【請求項 7 0】 ネットワークを介して保存要求されたデータを保存するための複数のサーバを備えたデータ保存サービス装置により実行される制御プログラムであって、

少なくともユーザのサービス加入条件のレベルに応じて選択した前記サーバに対して保存要求に係るデータを格納する内容を有することを特徴とする制御プログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ユーザのデータをインターネット等のネットワーク上のサーバにより保存するサービス技術に関する。

【0 0 0 2】

【従来の技術】

従来、電子写真やビデオストリーム等の情報は、広く公開することを目的としない限り、ユーザ側の機器（パソコン等の大容量ハードディスクや DVD、CD

ー R 等) でローカルに保存していた。

【 0 0 0 3 】

【発明が解決しようとする課題】

しかし、従来のように、ローカルに保存した場合、ユーザ側の機器が設置されている場所が火災・地震・台風等の災害により罹災したときに、大事な電子写真やビデオストリーム等の電子情報が失われてしまう虞がある。

【 0 0 0 4 】

そこで、この対策として、本出願人は、ユーザのデータをネットワーク上のサーバに保存するサービスシステムを提案している。このサービスシステムでは、火災・地震・台風等の災害が発生した場合、その災害が発生した地域のユーザのデータを優先的に安全度（対災害）の高いサーバに保存するようにしている。

【 0 0 0 5 】

しかし、上記サービスシステムでは、災害が発生した地域のユーザのデータを優先的に安全度（対災害）の高いサーバに保存する場合、保存要求順に保存処理を行っていた。このため、サービス契約金額が高いユーザ、サービス契約年数が長いユーザ等のサービス加入条件の高いユーザが、時間的に遅れて保存要求を行った場合は、その要求時点では既に安全度の高いサーバが満杯になっており、サービス加入条件の高いユーザが、安全度の低いサーバにしか保存して貰えなくなる、或いはサービスを全く受けられなくなる等の不具合が発生する可能性があった。

【 0 0 0 6 】

この問題を解決するためには、サーバの数を増やすことが考えられるが、サーバの数を増やした場合には、サービス提供者の運用経費が増大し、利益効率が低下してしまう。

【 0 0 0 7 】

本発明は、このような従来技術の問題に鑑みてなされたもので、その課題は、利益効率を低下させることなく、公平なデータ保存サービスを提供できるようにすることにある。

【 0 0 0 8 】

【課題を解決するための手段】

上記課題を解決するため、本発明は、ネットワークを介して保存要求されたデータを保存するための複数のサーバを備えたデータ保存サービス装置において、少なくともユーザのサービス加入条件のレベルに応じて前記サーバを選択する選択手段と、前記選択手段により選択されたサーバに対して保存要求に係るデータを格納する格納制御手段とを含むサービス制御手段を有している。

【0009】

また、本発明は、ネットワークを介して保存要求されたデータを保存するための複数のサーバを備えたデータ保存サービス装置の制御方法において、少なくともユーザのサービス加入条件のレベルに応じて前記サーバを選択する選択工程と、前記選択工程により選択されたサーバに対して保存要求に係るデータを格納する格納制御工程とを含むサービス制御工程を有している。

【0010】

また、本発明は、ネットワークを介して保存要求されたデータを保存するための複数のサーバを備えたデータ保存サービス装置により実行される制御プログラムであって、少なくともユーザのサービス加入条件のレベルに応じて選択した前記サーバに対して保存要求に係るデータを格納する内容を有している。

【0011】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。

【0012】

図1は、本発明を適用したユーザデータ保存管理システムの概略構成を示すシステム構成図であり、本システムでは、ユーザのデータをネットワーク上のサーバに保存するサービスを行っている。

【0013】

図1において、11はユーザデータ保存管理サービスを提供するアプリケーションサーバ群、12は上記サービスを享受するためのクライアント端末群、13は地震・台風等の予報情報を提供する気象データベースであり、これらアプリケーションサーバ群11、クライアント端末群12、気象データベース13は、イ

ンターネット等のネットワーク 1 0 を介して接続されている。

【 0 0 1 4 】

アプリケーションサーバ群 1 1 は、ユーザデータ保存管理処理を統括するアプリケーション統括サーバ 1 1 1、ユーザデータを保存するデータサーバ 1 1 2、1 1 3 を有している。なお、図 1 では、データサーバは 2 つだけを図示しているが、実際には多数のデータサーバが存在している。

【 0 0 1 5 】

また、クライアント端末群 1 2 は、リモートプリンタ 1 2 1、有線端末 1 2 2、無線端末 1 2 3、ユーザ識別モジュール 1 2 4、デジタルカメラ 1 2 5 を含んでいる。リモートプリンタ 1 2 1 は、データサーバ 1 1 2、1 1 3 に保存されたユーザのデータをプリントアウトするのに利用される。また、有線端末 1 2 2、及び無線端末 1 2 3 は、デジタルカメラ 1 2 5 により撮影された画像データをデータサーバ 1 1 2、1 1 3 に保存する際の通信端末として利用される。

【 0 0 1 6 】

なお、リモートプリンタ 1 2 1 とデジタルカメラ 1 2 5 には、ユーザ識別モジュール 1 2 4 を装着することができる。このユーザ識別モジュール 1 2 4 としては、本実施形態では、IC カードを使用しており、具体的には、ISO 7 8 1 6 に準拠した端子付スマートカードを使用している。このユーザ識別モジュール 1 2 4 には、アプリケーション統括サーバ 1 1 1 により保存処理されたユーザデータの保存先を示すアドレス情報（データサーバ 1 1 2、1 1 3 のアドレス）、データサーバ 1 1 2、1 1 3 にユーザデータを暗号化して保存する際に利用された暗号鍵の情報等が、アプリケーション統括サーバ 1 1 1 から送信されて格納される。

【 0 0 1 7 】

図 2 は、上記デジタルカメラ 1 2 5 の機能ブロック図である。

【 0 0 1 8 】

図 2 において、1 5 0 1 は撮像部、1 5 0 2 は撮像部 1 5 0 1 にて撮像された画像を電子データ化する画像処理部、1 5 0 3 は電子画像データを所望の暗号アルゴリズム・鍵により暗号化並びに復号化する暗号処理部、1 5 0 4 は電子画像

データを可視画像データに変換する出力制御部である。

【 0 0 1 9 】

また、1505はデジタルカメラ125の制御を司る制御CPU、1506は電子データ化された画像データを蓄積・保存する着脱メモリユニット、1507はネットワーク端末(122, 123)とのローカルリンクの通信を司る通信インタフェース、1508は機器制御プログラムを格納するメモリ、1509はユーザ識別モジュール124として用いるICカードとの間の通信を司るICカードインタフェース、1510は出力制御部1504にて変換された可視画像データを表示するディスプレイである。

【 0 0 2 0 】

図3は、上記リモートプリンタ121の機能ブロック図である。

【 0 0 2 1 】

図3において、1601はスキャナやパーソナルコンピュータ等のローカル機器からの入力データを受付けるローカル入力インタフェース、1602は入力された電子画像データを処理に適したフォーマットに変換する画像処理部、1603は電子画像データを所望の暗号アルゴリズム・鍵により、暗号化並びに復号化する暗号処理部、1604は電子画像データを可視画像データに変換し、プリンタエンジン1610をコントロールする出力制御部である。

【 0 0 2 2 】

また、1605はリモートプリンタの制御を司る制御CPU、1606は電子画像データを蓄積・保存する着脱メモリユニット、1607はネットワーク10との通信を司る通信インタフェース、1608は機器制御プログラムを格納するメモリ、1609はユーザ識別モジュール124として用いるICカードとの間の通信を司るICカードインタフェース、1610は出力制御部1604のコントロールに従い印刷を行うプリンタエンジンである。

【 0 0 2 3 】

図4は、ユーザ識別モジュール124としてのICカードの論理階層モデルである。

【 0 0 2 4 】

図4において、1701はICカード論理ファイルの構造の最上位階層であるMF (Master File)、1702は最上位DF (Dedicate File) に関する情報を格納する要素ファイルとしての最上位EF (Elementary File) である。

【0025】

また、1703、1704は前記MF 1701の直下に存在する最上位DFであり、本実施形態では、これら最上位のDF (サービス提供者用DF) 1703、1704には、これらDF 1703、1704を識別するためのアプリケーションIDがサービス提供者毎に割当てられている。

【0026】

上記DF 1703、1704の下位には、ユーザデータ格納サービスに関わるDF 1705、1706が存在し、これらDF 1705、1706の下位には、本アプリケーションで利用される各種情報 (ユーザ認証関連情報、データサーバ情報、アドレス情報、暗号鍵情報等) が格納される各種のファイル1707~1712が存在している。なお、DF 1705、1706以下の階層のファイルには、各サービス提供者が提供するサービスメニュー毎に、アプリケーションIDが割当てられている。

【0027】

次に、サービス享受会員 (単にユーザともいう) からユーザデータ保存要求を受付けた際のアプリケーション統括サーバ111の処理を、図5~図6に基づいて説明する。なお、ここでは、サービス享受会員が通信端末122、又は123を介してデジタルカメラ125内の画像データをデータサーバ112、又は113に保存する例を想定している。

【0028】

アプリケーション統括サーバ111は、まず、会員の要求に従い、通信端末122、又は123とアプリケーション統括サーバ111との間の通信回線を設定する (図5のステップS701、図6の401)。

【0029】

次に、クライアント端末側 (デジタルカメラ125) に装着されているユーザ

識別モジュール 1 2 4 とアプリケーション統括サーバ 1 1 1 との間で、クライアント端末操作者が正規会員であるか否かを判定すべく、ユーザ認証処理を行う（図 6 の 4 0 2，図 5 のステップ S 7 0 2）。

【 0 0 3 0 】

ユーザ認証に成功すれば、ユーザ識別モジュール 1 2 4 上で認識しているユーザレベル（ユーザのアプリケーションサービス加入条件）とアプリケーション統括サーバ 1 1 1 上で認識しているユーザレベルの一致を確認する（図 5 のステップ S 7 0 3、図 6 の 4 0 3，4 0 4）。

【 0 0 3 1 】

ユーザ認証、ユーザレベル確認の双方に成功した場合には、保存要求に係るユーザデータの転送を受付ける（図 5 のステップ S 7 0 4、図 6 の 4 0 5）。一方、前記の何れかに失敗した場合は、ユーザ識別モジュール 1 2 4 に対して失敗原因を通知すると共に、クライアント端末との間の回線を切断した後（図 5 のステップ S 7 1 0）、1 処理単位を終了する。

【 0 0 3 2 】

保存要求に係るユーザデータの転送を受付けたアプリケーション統括サーバ 1 1 1 は、受信したユーザデータを受信バッファ 2 0（図 7 参照）に一旦格納し、この受信に係るユーザデータについてチェックサム等により転送エラーの有無を判定する（図 5 のステップ S 7 0 5）。その結果、転送エラーがあった場合には、クライアント端末側に保存要求に係るユーザデータの再送を要求し（図 5 のステップ S 7 0 7）、ステップ S 7 0 4 に戻って、当該データの再送を待ち受ける。

【 0 0 3 3 】

一方、転送エラーが無かった場合は、データが正常に転送された旨を通知すると共に、通信端末 1 2 2，又は 1 2 3 との間の回線を切断した後（図 5 のステップ S 7 0 6、図 6 の 4 0 7）、格納先データサーバの選定処理を行う（図 5 のステップ S 7 0 8）。そして、選定したデータサーバ 1 1 2，又は 1 1 3 に対するユーザデータの格納処理を行い（図 5 のステップ S 7 0 9）、そのデータ格納条件をユーザ識別モジュール 1 2 4 に通知して（図 5 のステップ S 7 1 1、図 6 の

4 0 8)、1 処理単位を終了する。

【 0 0 3 4 】

図 5 のステップ S 7 1 1 (図 6 の 4 0 8) におけるデータ格納条件の通知処理では、選定したデータサーバ 1 1 2, 又は 1 1 3 (後述の第 1、又は第 2 のデータサーバ) へのユーザデータ格納の結果 (成功、失敗) 及び、第 1、第 2 のデータサーバの識別情報 (I P アドレス等)、ユーザデータ格納時に用いた暗号化アルゴリズム、及び暗号化鍵の情報等のデータ格納条件に関わる各種の情報が、非リアルタイムの通信手段 (電子メールへの添付等) を用いて通信端末 1 2 2, 1 2 3 経由でユーザ識別モジュール 1 2 4 に通知されて格納される。

【 0 0 3 5 】

なお、本実施形態では、アプリケーション統括サーバ 1 1 1 と通信端末 1 2 2, 又は 1 2 3 との間の通信に用いられる通信回線として、接続時間課金方式の通信回線を利用することを想定しているため、データ格納条件に関わる情報を非リアルタイムの通信手段を用いてユーザ識別モジュール 1 2 4 に通知すべく、一旦通信回線を切断した後にデータ格納条件を通知するようにしている。

【 0 0 3 6 】

しかし、アプリケーション統括サーバ 1 1 1 と通信端末 1 2 2, 又は 1 2 3 との間の通信回線の切断処理を、データ格納条件の通知処理の後に行ってもよい。この場合には、ユーザ識別モジュール 1 2 4 上でのデータ格納条件の変更を、アプリケーション統括サーバ 1 1 1 側で迅速に確認できるようになる。特に、通信回線が通信データ量による課金方式である場合は、後述の方式の方が前述の方式よりも利便性が高くなる。

【 0 0 3 7 】

次に、図 5 のステップ S 7 0 8 における格納先データサーバの選定処理を、図 8 のフローチャートに基づいて詳細に説明する。

【 0 0 3 8 】

本選定処理では、アプリケーション統括サーバ 1 1 1 は、まず、今回アクセスしてきたユーザ (会員) のユーザプロフィールを参照して、当該ユーザの居住地情報等を認識すると共に (図 8 のステップ S 8 0 1)。当該ユーザのユーザレベ

ル（契約料金プランや契約継続年数等）を認識する（図 8 のステップ S 8 0 2）

【 0 0 3 9 】

次に、ユーザレベル毎の罹災リスクテーブル（図 1 1 の処理にて、ユーザレベル情報・罹災リスク情報に変更が生じる度に更新される）を参照し（図 8 のステップ S 8 0 3）、当該ユーザレベルにおける罹災リスクテーブル上で最も罹災リスクの低いデータサーバを第 1 のデータ格納サーバとして選定し、当該ユーザレベルにおける罹災リスクテーブル上で、当該ユーザの居住地以外（居住地から十分な物理的な距離が確保される場所）に存在するものの中で、最も罹災リスクの低いデータサーバ（ただし、第 1 のデータ格納サーバの選定結果と同一になってしまった際には、2 番目に罹災リスクの低いデータサーバ）を第 2 のデータ格納サーバとして選定する（図 8 のステップ S 8 0 4）。

【 0 0 4 0 】

そして、選定した各データサーバにデータを格納する際に用いる暗号方式と、暗号鍵を選定する（図 8 のステップ S 8 0 5）。

【 0 0 4 1 】

次に、図 5 のステップ S 7 0 9 におけるデータサーバへのデータ格納処理を、図 7、図 9、及び図 1 0 に基づいて詳細に説明する。

【 0 0 4 2 】

本格納処理では、アプリケーション統括サーバ 1 1 1 は、まず、選定した第 1 のデータ格納サーバを指定し（図 1 0 の 5 0 1）、この第 1 のデータ格納サーバの認証を行い（図 1 0 の 5 0 2）、成りすまし等の不正サーバでないことを確認する（図 9 のステップ S 1 0 0 1）。

【 0 0 4 3 】

そして、第 1 のデータ格納サーバが正当なデータサーバであると確認された場合は、保存要求に係るユーザデータを先のサーバ選定時に選択した当該第 1 のデータサーバ用の暗号鍵 A と暗号アルゴリズム（図 7 の 2 2）を用いて暗号化した後、当該第 1 のデータ格納サーバに暗号化済みのデータを転送する（図 1 0 の 5 0 3、図 9 のステップ S 1 0 0 2）。そして、第 1 のデータ格納サーバからデー

タ転送確認応答が得られたか否かを判別する（図9のステップS1003、図10の504）。その結果、データ転送確認応答が得られなかった場合は、データ転送に失敗したものとして、ステップS1002に戻り、データを再送する。

【0044】

一方、データ転送確認応答が得られた場合は、ステップS1004に進む。また、ステップS1001にて、正当なデータサーバと確認出来なかった場合は、不正データサーバ検出処理を行って（ステップS1007）、ステップS1004に進む。なお、この不正データサーバ検出処理については、後で図17のフローチャートに基づいて詳細に説明する。

【0045】

ステップS1004では、選定した第2のデータ格納サーバを指定し（図10の505）、この第2のデータ格納サーバの認証を行い（図10の506）、成りすまし等の不正サーバでないことを確認する。

【0046】

そして、第2のデータ格納サーバが正当なデータサーバであると確認された場合は、保存要求に係るユーザデータを先のサーバ選定時に選択した当該第2のデータサーバ用の暗号鍵Bと暗号アルゴリズム（図7の23）を用いて暗号化した後、当該第2のデータ格納サーバに暗号化済みのデータを転送する（図10の507、図9のステップS1005）。そして、第2のデータ格納サーバからデータ転送確認応答が得られたか否かを判別する（図9のステップS1006、図10の508）。その結果、データ転送確認応答が得られなかった場合は、データ転送に失敗したものとして、ステップS1005に戻り、データを再送する。

【0047】

一方、データ転送確認応答が得られた場合は、1処理単位を終了する。また、ステップS1004にて、正当なデータサーバと確認出来なかった場合は、不正データサーバ検出処理を行って（ステップS1008）、1処理単位を終了する。なお、この不正データサーバ検出処理については、後で図17のフローチャートに基づいて詳細に説明する。

【0048】

以上のような処理により、アプリケーション享受会員にとっては、データ格納場所を指定するための特段の操作を行わなくても、会員の居住地以外の場所、地震・台風等の災害による罹災の可能性が低い場所にあるデータサーバに、所望のユーザデータを保存することができるため、会員宅の罹災や会員の居住地域で発生した災害による物理的ダメージから、大事なユーザデータを保護することが可能となる。

【0049】

また、ユーザデータ格納アプリケーション提供者にとっては、会員のレベル（加入料金プランや継続契約年数等）をデータサーバ選択の際のパラメータとして加味することにより、ユーザレベルに応じた公平なデータ保存サービスをユーザに提供することが可能となると共に、データサーバの数を増やさなくても、データサーバが満杯になるのを可及的に回避することができ、利益効率の高いデータ保存サービスを提供することが可能となる。

【0050】

次に、ユーザレベル毎の罹災リスクテーブルの更新処理を、図11のフローチャートに基づいて説明する。なお、この罹災リスクテーブルの更新処理は、アプリケーション統括サーバ111により、定期的に自動的に実行されるものである。

【0051】

本更新処理では、アプリケーション統括サーバ111は、まず、各ユーザについて、ユーザプロファイルを参照してユーザレベル情報の変化の有無を判別すると共に（ステップS901）、気象データベース13を参照して罹災リスク情報の変化の有無を判別する（ステップS902）。その結果、ユーザレベル情報、罹災リスク情報の何れも変化していない場合は、そのまま、1処理単位を終了する。

【0052】

ユーザレベル情報、罹災リスク情報の少なくとも一方が変化している場合は、その変化した情報に基づいて、ユーザレベル毎の罹災リスクテーブルの情報を更新する（ステップS903）。そして、そのテーブル更新に応じて格納データサ

ーバを変更する必要があるか否かを判別し（ステップ S 9 0 4）、格納データサーバを変更する必要がなければ、1 処理単位を終了する。

【 0 0 5 3 】

一方、格納データサーバを変更する必要があるれば、前述の図 8 のフローチャートに基づいて、格納データサーバを選定し直す（ステップ S 9 0 5）。そして、前述の図 9 のフローチャートに基づいて、選定し直した格納データサーバに対してユーザデータを格納し直す（ステップ S 9 0 6）。

【 0 0 5 4 】

次に、格納し直しに伴って変化したデータ格納条件を、非リアルタイムの通信手段（電子メールへの添付等）を用いて、通信端末 1 2 2、1 2 3 経由でユーザ識別モジュール 1 2 4 に通知することにより格納させて（ステップ S 9 0 7）、1 処理単位を終了する。

【 0 0 5 5 】

このように、データサーバに一旦保存したユーザデータについては、その後、ユーザレベルや罹災リスクが変化したとしても、その変化に応じて自動的に格納データサーバの再選定・再格納処理が行われるので、質の高いサービスを提供することが可能となる。

【 0 0 5 6 】

次に、データサーバ 1 1 2、1 1 3 に保存中のユーザデータ（電子写真情報等）を読み出し、リモートプリンタ 1 2 1 で出力する際の通信処理を、図 1 2 のフローチャート、及び図 1 3 のシーケンス図に基づいて説明する。

【 0 0 5 7 】

リモートプリンタ 1 2 1 は、本リモートプリンタ 1 2 1 に装着されているユーザ識別モジュール 1 2 4 から、ユーザデータが格納されているデータサーバに関する各種の情報（アクセスのためのアドレス、利用暗号化鍵、利用暗号化アルゴリズム等）を読み出す（図 1 3 の 6 0 1）。なお、ユーザは、リモートプリンタ 1 2 1 を操作することにより、出力したいユーザデータを予め選択しておく（図 1 2、図 1 3 には記述なし）。

【 0 0 5 8 】

リモートプリンタ 1 2 1 は、選択されたユーザデータが格納されているデータサーバ（ここではデータサーバ 1（1 1 2））との間の通信回線を設定する（図 1 2 のステップ S 1 4 0 1、図 1 3 の 6 0 2）。次に、回線接続したデータサーバ 1 1 2 とユーザ識別モジュール 1 2 4 との間でユーザ認証処理を行う（図 1 2 のステップ S 1 4 0 2、図 1 3 の 6 0 3）。ユーザ認証に失敗した場合は、このまま回線を切断して（図 1 2 のステップ S 1 4 0 6）、ユーザデータ読み出し処理を終了する。

【 0 0 5 9 】

一方、ユーザ認証に成功した場合は、データサーバ 1 1 2 からのユーザデータを受け取り（図 1 2 のステップ S 1 4 0 3、図 1 3 の 6 0 4）、チェックサム等により転送エラーの有無を判定する（図 1 2 のステップ S 1 4 0 4、図 1 3 の 6 0 5）。転送エラーが発生していた場合は、当該ユーザデータの再送を要求して（図 1 2 のステップ S 1 4 0 7）、ステップ S 1 4 0 3 に戻る。

【 0 0 6 0 】

一方、転送エラーが発生していなかった場合は、利用暗号化鍵、利用暗号化アルゴリズムを用いて転送データを復号する（図 1 2 のステップ S 1 4 0 5）。そして、回線を切断して（図 1 2 のステップ S 1 4 0 6、図 1 3 の 6 0 6、6 0 7）、ユーザデータの読出し処理を終了する。

【 0 0 6 1 】

次に、保存データの正当性の確認処理を、図 1 4 ～図 1 7 に基づいて説明する。なお、この保存データの正当性の確認処理は、アプリケーション統括サーバ 1 1 1 により定期的に実行されるものである。

【 0 0 6 2 】

まず、アプリケーション統括サーバ 1 1 1 は、当該アプリケーション統括サーバ 1 1 1 内のアプリケーション享受会員情報記憶エリア（図 1 5 の 3 1）より、今回、データの正当性確認を行う会員のユーザデータ（電子写真情報）が格納されているデータサーバ（第 1、第 2 の格納データサーバ）に関する情報（格納データサーバのアドレス、利用暗号鍵情報等）を読出し、その情報に基づいて、第 1 の格納データサーバ、第 2 の格納データサーバについて、サーバ認証処理を行

う（図14のステップS1101, S103）。

【0063】

第1の格納データサーバ、第2の格納データサーバの少なくとも一方について、サーバ認証に失敗した場合は、不正データサーバ検出処理を行い（図14のステップS1107）、1処理単位を終了する。なお、不正データサーバ検出処理については、図17に基づいて、後で詳細に説明する。

【0064】

一方、第1の格納データサーバ、第2の格納データサーバの双方ともサーバ認証に成功した場合は、そのサーバ認証に成功した第1の格納データサーバ、及び第2の格納データサーバ内の暗号化に係るユーザデータを、アプリケーション統括サーバ111に取り込む（図14のステップS1102, S1104）。

【0065】

そして、取り込んだ暗号化に係るユーザデータを、対応する暗号鍵、アルゴリズムを用いて復号して（図14のステップS1105、図15の32, 33）、両方のユーザデータが一致しているか否かを判別する（図14のステップS1106）。その結果、両方のユーザデータが一致している場合は、そのまま1処理単位を終了する。一方、一致していない場合は、ユーザデータ改竄検出処理を行って（図14のステップS1108）、1処理単位を終了する。

【0066】

次に、図14のステップS1108におけるユーザデータ改竄検出処理を、図16のフローチャートに基づいて詳細に説明する。

【0067】

本ユーザデータ改竄検出処理では、アプリケーション統括サーバ111は、比較対象のデータサーバ112, 113の双方に対して、当該ユーザ（同一のユーザ）に係るユーザデータ記憶エリアのディスク（メモリ）スキャン（ローカルチェック）を指示する（ステップS1201）。この指示を受けた各データサーバ112, 113では、ユーザデータ記憶エリアのエラー検出処理を行うと共に、エラー箇所の補正が可能であれば訂正処理を行い、各処理結果をアプリケーション統括サーバ111に通知する。

【 0 0 6 8 】

そこで、アプリケーション統括サーバ 1 1 1 は、データサーバ 1 1 2, 1 1 3 によるエラー補正の有無を判別し（ステップ S 1 2 0 2）、エラー補正がなされていた場合には、再度、図 1 4 の格納データの正当性確認処理を行う（ステップ S 1 2 0 3）。

【 0 0 6 9 】

一方、エラー補正がなされていない場合には、ユーザデータの改竄が第三者によりなされたものと判断し、双方のユーザデータの相違箇所情報を、参照可能情報格納エリア 3 0（図 1 5 の 3 2）に格納した後、通信端末経由でユーザに通知する（ステップ S 1 2 0 4）。

【 0 0 7 0 】

次に、図 1 4 のステップ S 1 1 0 7 における不正データサーバ検出処理を、図 1 7 のフローチャートに基づいて詳細に説明する。

【 0 0 7 1 】

不正データサーバを検出した時点において、データサーバへのユーザデータの書き込み処理中であった場合は、クライアントユーザ（会員）との通信回線の設定処理をアプリケーション統括サーバ 1 1 1 側が起動する（ステップ S 1 3 0 1, S 1 3 0 2）。そして、アプリケーション統括サーバ 1 1 1 は、ユーザ識別モジュール 1 2 4 との間でユーザ認証を行い（ステップ S 1 3 0 3）、ユーザ認証に失敗した場合は、クライアントユーザ（会員）との通信回線を切断して（ステップ S 1 3 0 9）、1 処理単位を終了する。

【 0 0 7 2 】

一方、ユーザ認証に成功した場合は、図 8 のフローチャートに基づいて格納データサーバを選定し直す（ステップ S 1 3 0 4）。ただし、ここでの選定処理においては、不正サーバとして検出されたデータサーバの格納データサーバとしての選択優先順位は、下げた状態で選定処理を行う。次に、アプリケーション統括サーバ 1 1 1 は、クライアントユーザ（会員）との通信回線を切断し（ステップ S 1 3 0 5）、選定し直したデータサーバへのデータ格納処理を図 9 のフローチャートに基づいて行い（ステップ S 1 3 0 6）、1 処理単位を終了する。

【0073】

ステップS1301にて、不正データサーバを検出した時点では、データサーバへの書込処理を行っていなかったと判別された場合は、当該検出されたデータサーバについて、不正サーバとしての検出回数が規定回数以上（1回以上で任意の値に設定可能）であるか否かを判別する（ステップS1307）。その結果、不正サーバとしての検出回数が規定回数以上でなければ、そのまま1処理単位を終了し、規定回数以上であれば、クライアント端末経由で会員に通知して（ステップS1308）、1処理単位を終了する。なお、この通知は、本実施形態では、電子メール等の非リアルタイム通信を想定している。

【0074】

このように、アプリケーション統括サーバ111が自律的、定期的にデータサーバ上のユーザデータの正当性をチェックすることにより、アプリケーション享受会員が、データサーバ上に保存している電子写真情報等のユーザデータの正当性（改竄がない等）を確認するための手間を大幅に軽減することが可能となる。

【0075】

図18は、本ユーザデータ保存管理システムにおける会員への課金（アプリケーションサービス享受対価の支払）処理を説明するための模式図である。

【0076】

図18において、111は図1等にしたアプリケーション統括サーバ、112、113は図1にしたデータサーバである。また、1803は本アプリケーションサービスを提供している事業者（以下、サービス提供者という）の取引金融機関の情報サーバ、1804は会員（本アプリケーションサービス享受者：以下、ユーザという）の取引金融機関の情報サーバ、10は図1にしたネットワーク、181は金融機関専用ネットワーク（クローズネットワーク）である。

【0077】

次に、図19のフローチャートに基づいて、図18を適宜参照しながら、アプリケーション統括サーバ111の会員に対する課金処理を説明する。

【0078】

会員への課金の決算日（図18の1810）が到来すると、アプリケーション

統括サーバ 1 1 1 は、課金決算対象のユーザ毎に格納に係るユーザデータの妥当性を、図 1 4 のフローチャートに基づいて確認する（図 1 8 の 1 8 1 1、図 1 9 のステップ S 1 9 0 1）。その結果、ユーザデータの妥当性が確認された場合は、課金決算対象のユーザ毎に、今期のデータ保存に対する対価をユーザレベル、データ改竄の有無等の各種条件に基づいて算出する（ステップ S 1 9 0 2）。

【 0 0 7 9 】

一方、ユーザデータの妥当性が確認できなかった場合は、図 8 のフローチャートに基づいて格納対象データサーバの再選定処理を行い（ステップ S 1 9 0 3）、図 9 のフローチャートに基づいて再選定に係るデータサーバへのユーザデータの格納処理を行った後に（ステップ S 1 9 0 4）、課金決算対象のユーザ毎に、今期のデータ保存に対する対価をユーザレベル、データ改竄の有無等の各種条件に基づいて算出する（ステップ S 1 9 0 2）。

【 0 0 8 0 】

次に、前記ユーザ毎に、今期のデータ保存に対する対価と最新のデータ格納サーバの情報（IP アドレス、暗号アルゴリズム、暗号鍵、障害履歴、不服申し立て期限日・方法、等）を、ネットワーク 1 0 を介して、非リアルタイム通信手段（電子メールの添付ファイル等）を用いて通知する（図 1 8 の 1 8 1 3、図 9 のステップ S 1 9 0 5）。なお、前記通知（メール）は、ネットワーク 1 0 に接続された通信端末 1 2 2、1 2 3 にて受信して確認することができる。また、通信端末 1 2 2、1 2 3 にユーザ識別モジュール 1 2 4 を装着して、受信に係るメールをユーザ識別モジュール 1 2 4 に格納することもできる。

【 0 0 8 1 】

ユーザは、万一、内容（課金額や障害履歴等）に不服がある場合は、通知に係る不服申し立て方法に従って、期限日までにサービス提供者に対して不服を申し立てることができる。そこで、アプリケーション統括サーバ 1 1 1 は、不服申し立て期限日が経過する迄に、ユーザからの不服申し立てがあったか否かを判別する（ステップ S 1 9 0 6）。

【 0 0 8 2 】

その結果、不服申し立てが無ければ、サービス提供者の取引金融機関情報サー

バ 1 8 0 3 に対して、当該ユーザの金融機関の口座より、決済日に指定の金額を引き落とすべき旨を通知して（図 1 8 の 1 8 1 2，図 1 9 のステップ S 1 9 0 7）、1 処理単位を終了する。一方、不服申し立てがあった場合は、当該ユーザのユーザプロフィール等の再確認処理を行い（ステップ S 1 9 0 8）、ステップ S 1 9 0 6 に戻り、再度、ユーザからの不服申し立ての有無を確認する。

【 0 0 8 3 】

課金の決済日には、サービス提供者の取引金融機関情報サーバ 1 8 0 3 から当該ユーザの取引金融機関情報サーバ 1 8 0 4 に対して支払金額と支払先口座の指定を行う（図 1 8 の 1 8 2 1）。この指定を受付けた当該ユーザの取引金融機関情報サーバ 1 8 0 4 は、指定の支払額を指定の支払口座に支払うと共に（図 1 8 の 1 8 2 2）、当該ユーザに対して、非リアルタイム通信手段（電子メールの添付ファイル等）を用いてサービスの享受対価の支払を終えた旨、及び支払履歴を通知することにより（図 1 8 の 1 8 2 3）、支払履歴をユーザ識別モジュール 1 2 4 に格納させる。

【 0 0 8 4 】

以上の処理によって、ユーザデータ保存管理システム上で、サービス提供者とユーザとの間での合意が取れた課金処理を実現することが可能となる。また、課金情報、格納データサーバ等の各種情報、取引金融機関からの支払い情報等のユーザ毎の情報をアプリケーション統括サーバ 1 1 1、ユーザ識別モジュール 1 2 4 の双方で管理しているので、上記の各種情報をユーザ側からも確認することが可能となり、保存データ等の改竄を確実に検知することが可能となる。

【 0 0 8 5 】

なお、本発明は、上記実施形態に限定されることなく、例えば、電子写真情報以外のテキスト情報、ビデオストリーミング情報（電子動画情報）、音声情報等を保存管理することも可能である。また、ユーザ識別モジュールとしては、IC カード（ISO 7 8 1 6 規定の端子付 IC カード）を用いることなく、非接触式の IC カードを用いることも可能である。さらに、携帯電話機・携帯情報端末等に、ユーザ識別モジュール自体を一体に組み込み、或いはユーザ識別モジュールと同等の機能を搭載することにより、ユーザ識別モジュールを端末に装着する手

間を省くことも可能である。

【0086】

また、罹災リスクの判定処理については、気象データサーバ13の地震予知情報、台風情報等を利用して行うだけでなく、損害保険会社等で管理している損害保険（火災保険・地震保険等）の地域毎の料率情報を利用して行うことも可能である。また、銀行間の専用ネットワークシステム（クローズネットワーク）を利用した口座振替処理による課金・決済方式ではなく、汎用ネットワーク（オープンネットワーク）上の暗号通信を通信媒体として用いるデビットカード・クレジットカードシステムによる課金・決済方式を用いることも可能である。

【0087】

さらに、ユーザ識別モジュール124上に、電子現金（金融機関統括サーバの承認無しで価値の移動が可能な電子マネー）アプリケーションが実装されていれば、支払額の通知を受取ったユーザが、アプリケーション統括サーバ111に電子現金を汎用ネットワーク（オープンネットワーク）上の暗号通信を通信媒体として用いて送付することにより、前記金融機関サーバを介さずに、直接決済を行うことも可能である。

【0088】

【発明の効果】

以上説明したように、本発明によれば、少なくともユーザのサービス加入条件のレベルに応じて選択したサーバに対して保存要求に係るデータを格納するようにしているので、利益効率を低下させることなく、公平なデータ保存サービスを提供することが可能となる。

【図面の簡単な説明】

【図1】

本発明を適用したユーザデータ保存管理システムの概略構成を示すシステム構成図である。

【図2】

クライアント端末としてのデジタルカメラの機能ブロック図である。

【図3】

クライアント端末としてのリモートプリンタの機能ブロック図である。

【図 4】

ユーザ識別モジュールの論理情報の記憶階層モデルを示す概念図である。

【図 5】

クライアント端末から接続要求（ユーザデータ保存要求）を受けた場合のアプリケーション統括サーバの処理を示すフローチャートである。

【図 6】

クライアント端末から接続要求（ユーザデータ保存要求）がなされた場合の通信処理を示すシーケンス図である。

【図 7】

クライアント端末から接続要求（ユーザデータ保存要求）を受けた場合のアプリケーション統括サーバの処理を説明するための概念図である。

【図 8】

アプリケーション統括サーバによるユーザデータ格納用のデータサーバの選定処理を示すフローチャートである。

【図 9】

選定に係るデータサーバへのアプリケーション統括サーバによるユーザデータの格納処理を示すフローチャートである。

【図 1 0】

選定に係るデータサーバへのユーザデータの格納処理時の通信処理を示すシーケンス図である。

【図 1 1】

アプリケーション統括サーバによるユーザレベル毎の罹災リスクテーブルの更新処理を示すフローチャートである。

【図 1 2】

リモートプリンタによるデータサーバからのユーザデータのダウンロード処理を示すフローチャートである。

【図 1 3】

データサーバからのユーザデータのダウンロード処理を行う場合の通信処理を

示すシーケンス図である。

【図14】

アプリケーション統括サーバによるデータサーバ内のユーザデータの正当性の確認処理を示すフローチャートである。

【図15】

アプリケーション統括サーバによるデータサーバ内のユーザデータの正当性の確認処理を説明するための概念図である。

【図16】

アプリケーション統括サーバによるユーザデータの改竄検出処理を示すフローチャートである。

【図17】

アプリケーション統括サーバによる不正データサーバ検出処理を示すフローチャートである。

【図18】

クローズネットワーク（専用網）を併用した課金処理を説明するための模式図である。

【図19】

アプリケーション統括サーバによる上記課金処理を示すフローチャートである。

【符号の説明】

- 10：ネットワーク
- 11：アプリケーションサーバ群
- 12：クライアント端末群
- 13：気象データベースサーバ
- 111：アプリケーション統括サーバ
- 112：第1のデータサーバ
- 113：第2のデータサーバ
- 121：リモートプリンタ
- 122：有線通信端末

1 2 3 : 無線通信端末

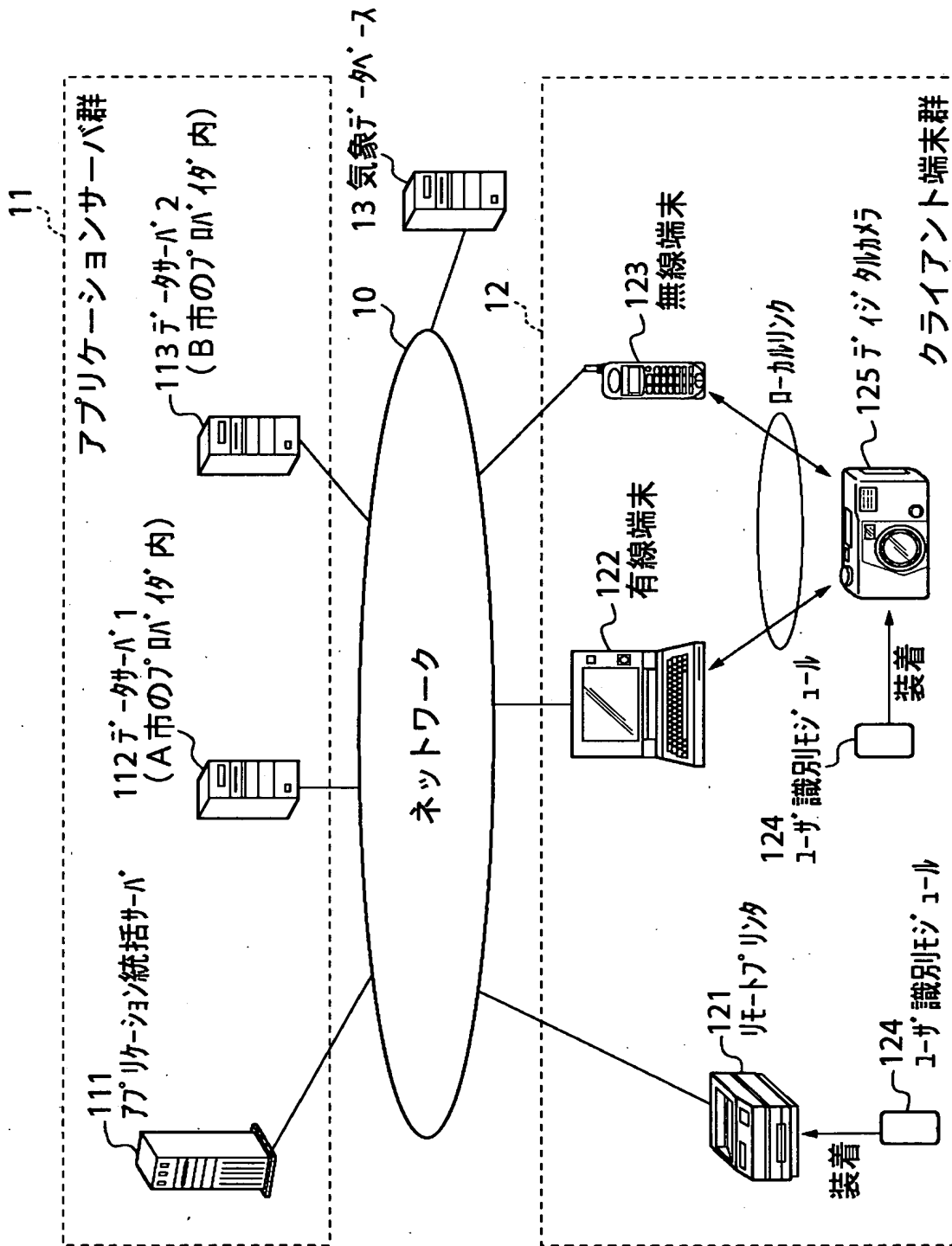
1 2 4 : ユーザ識別モジュール

1 2 5 : デジタルカメラ

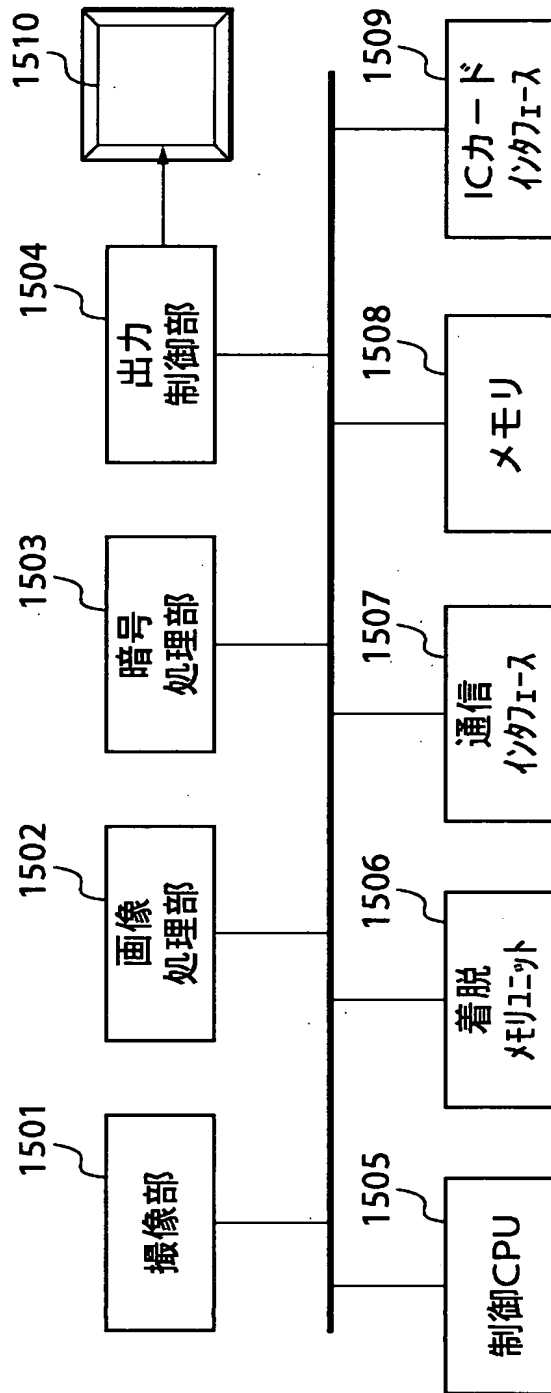
【書類名】

図面

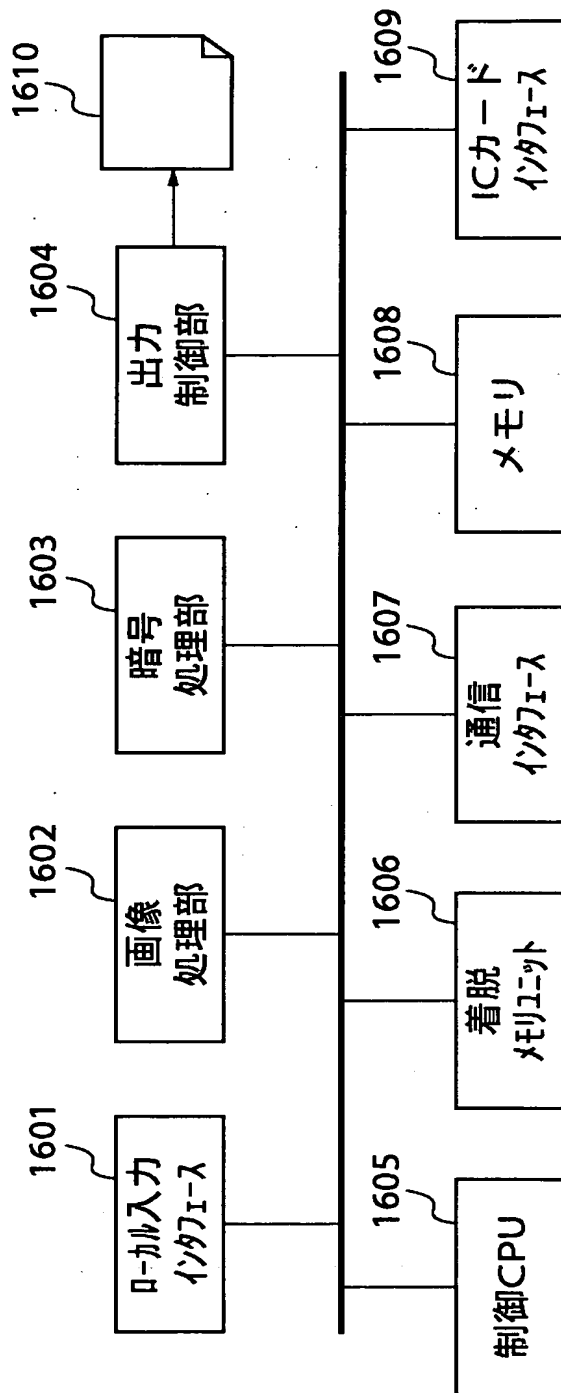
【図 1】



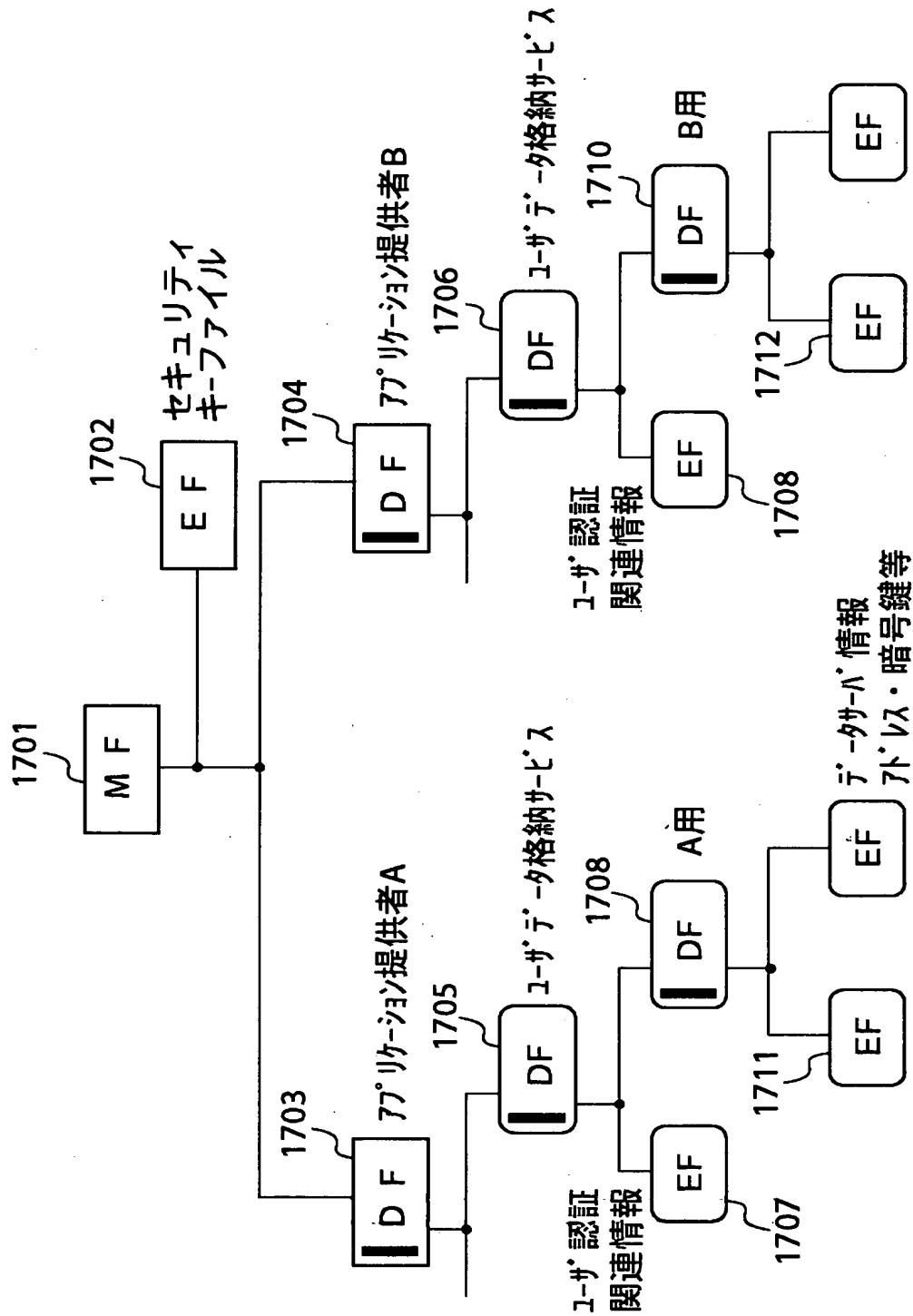
【図 2】



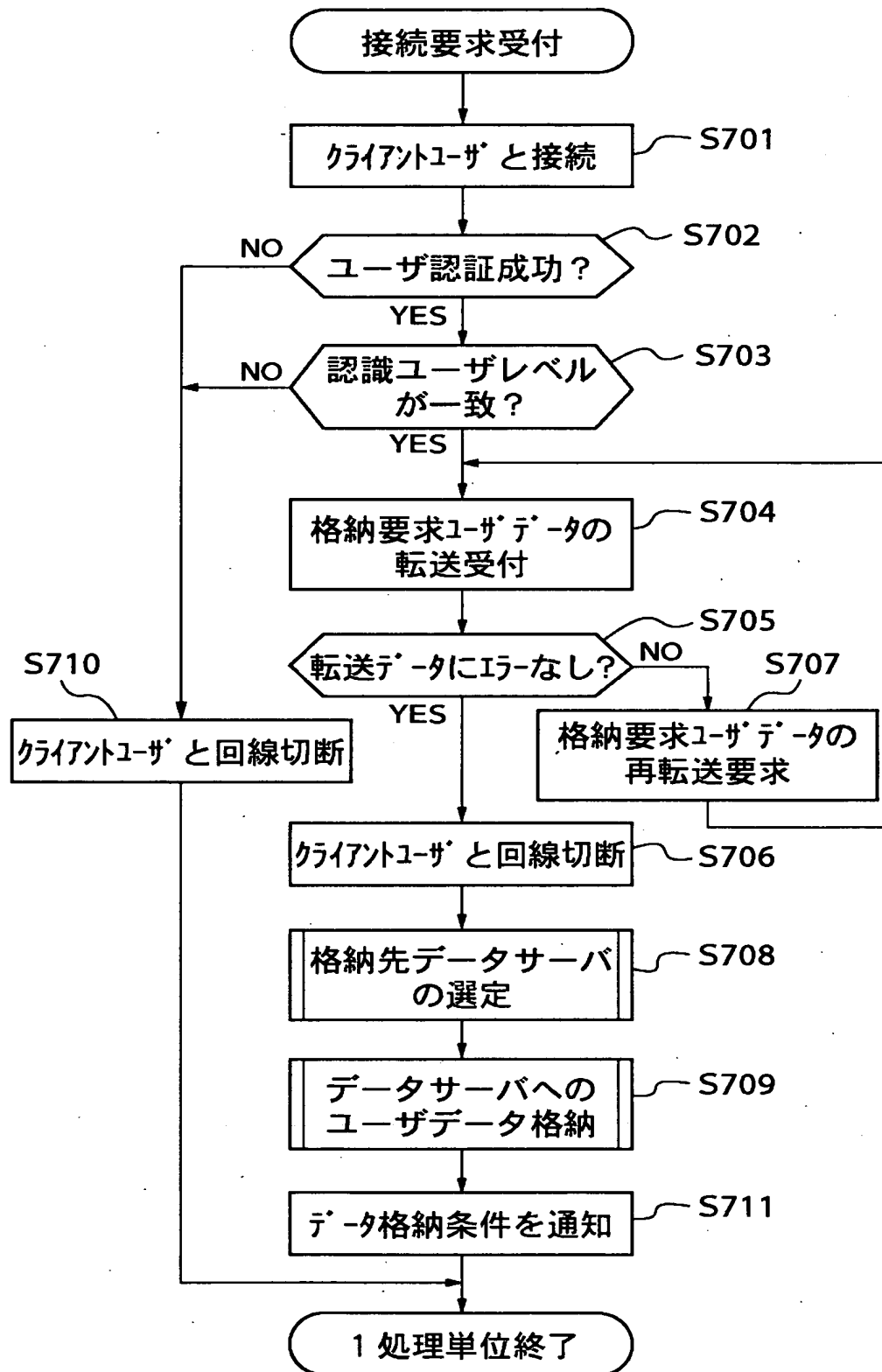
【図 3】



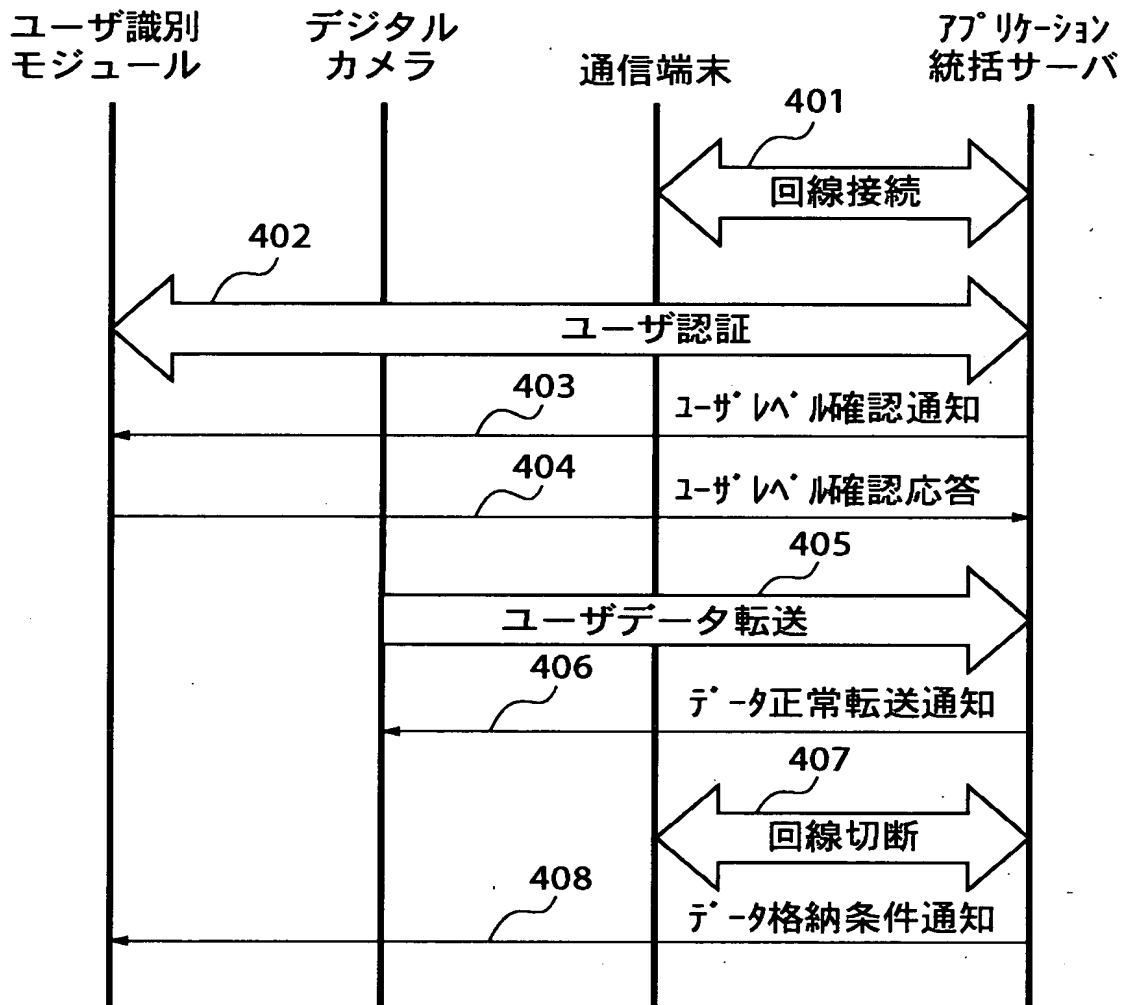
【図4】



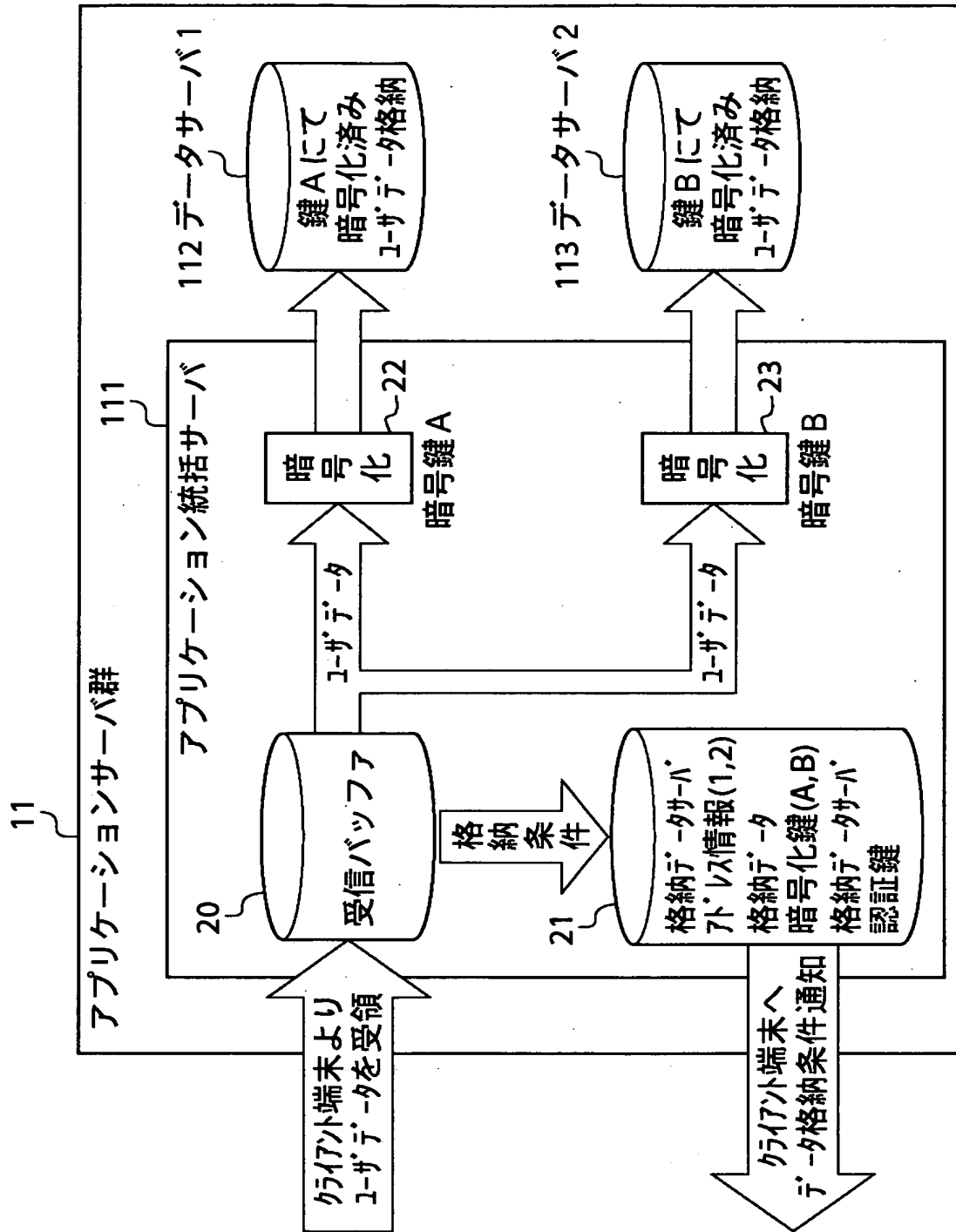
【図 5】



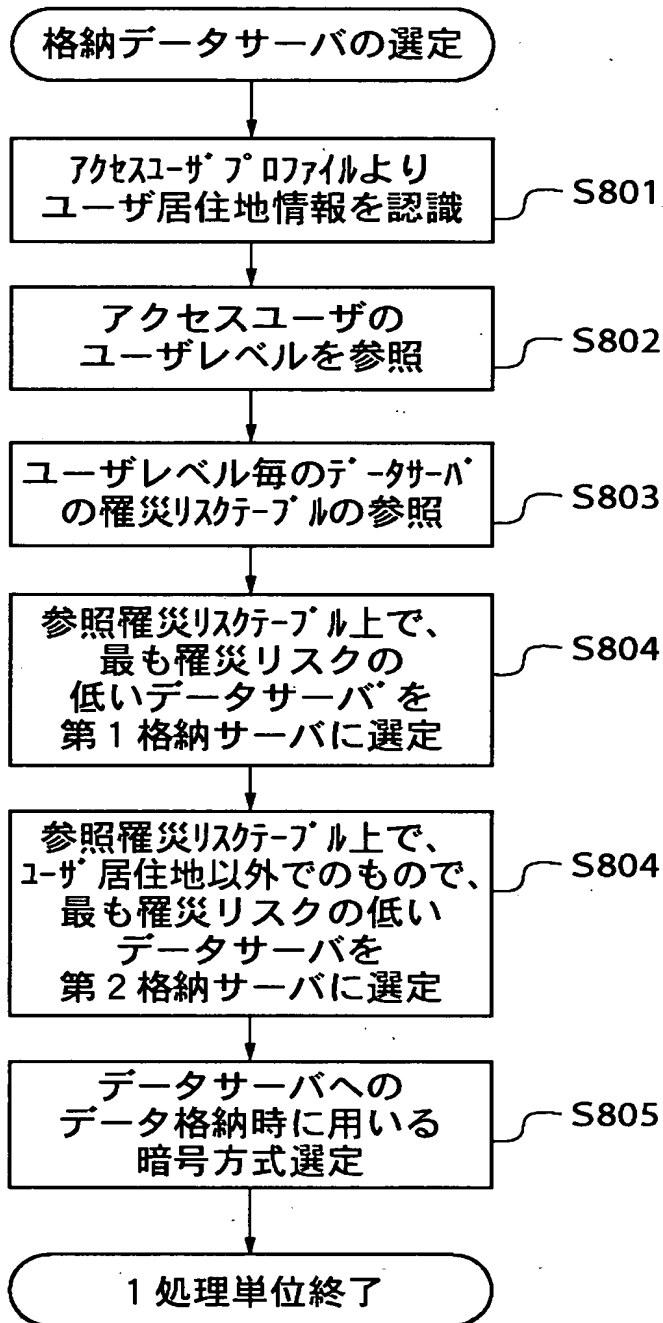
【図 6】



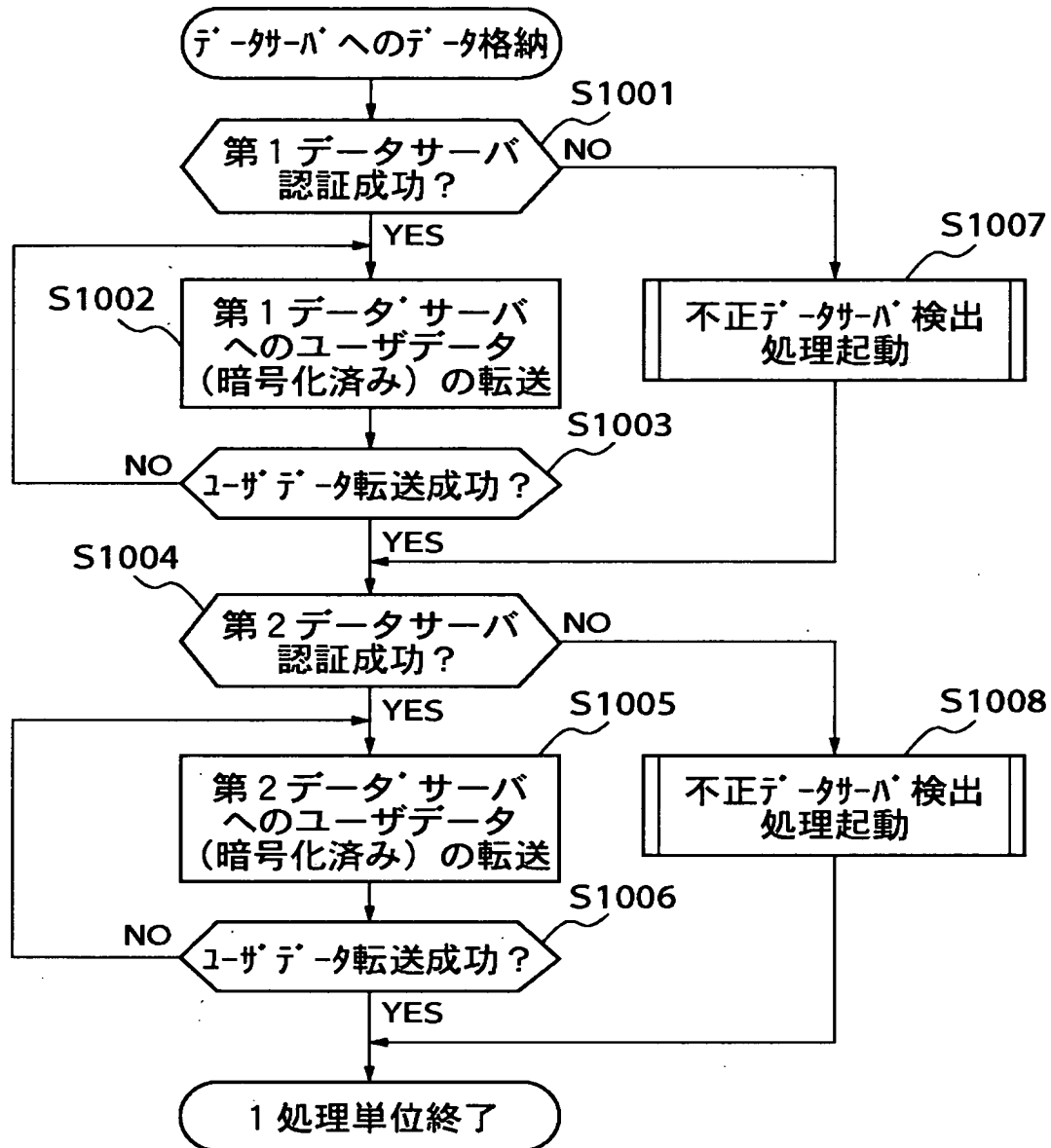
【図 7】



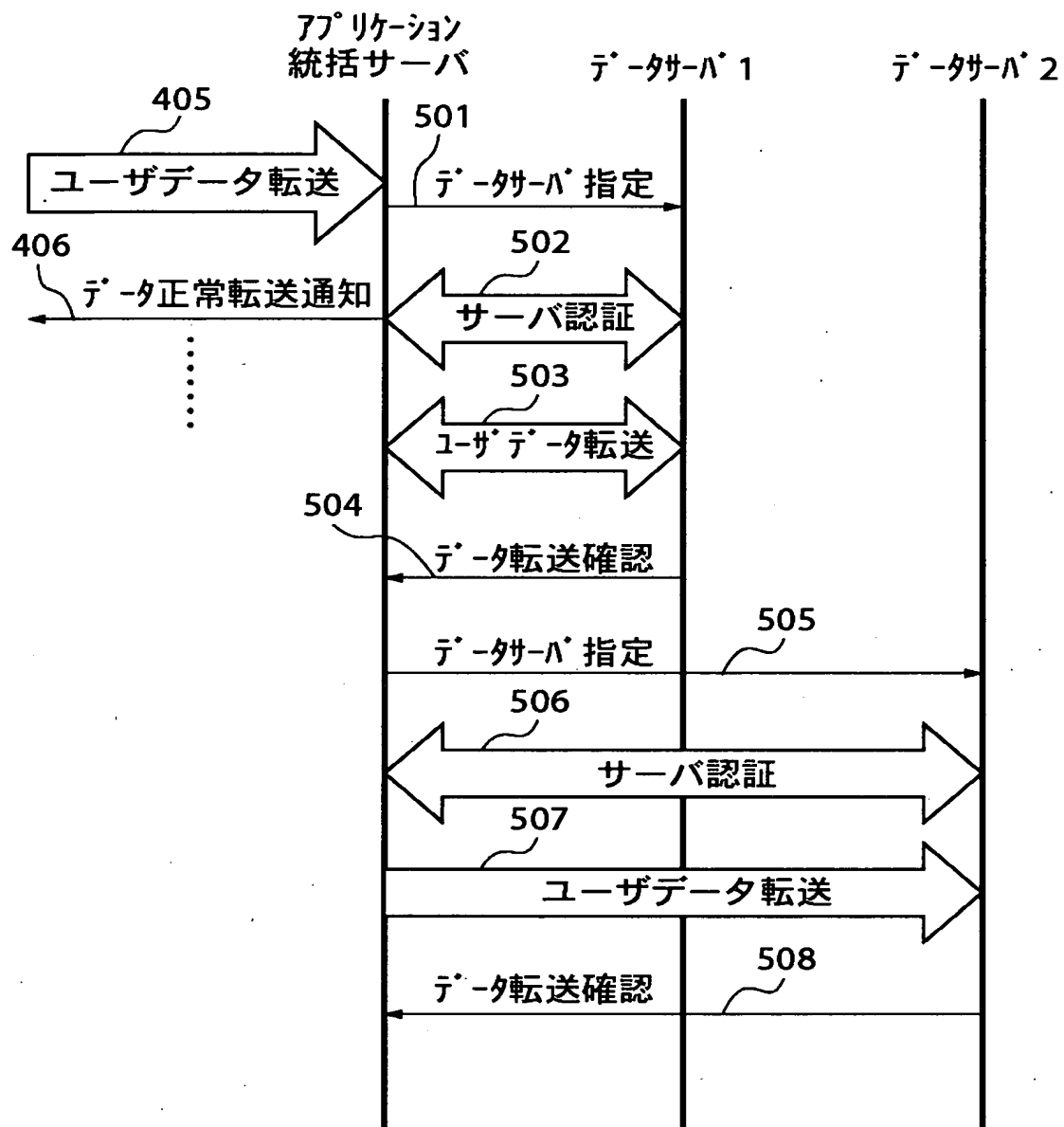
【図 8】



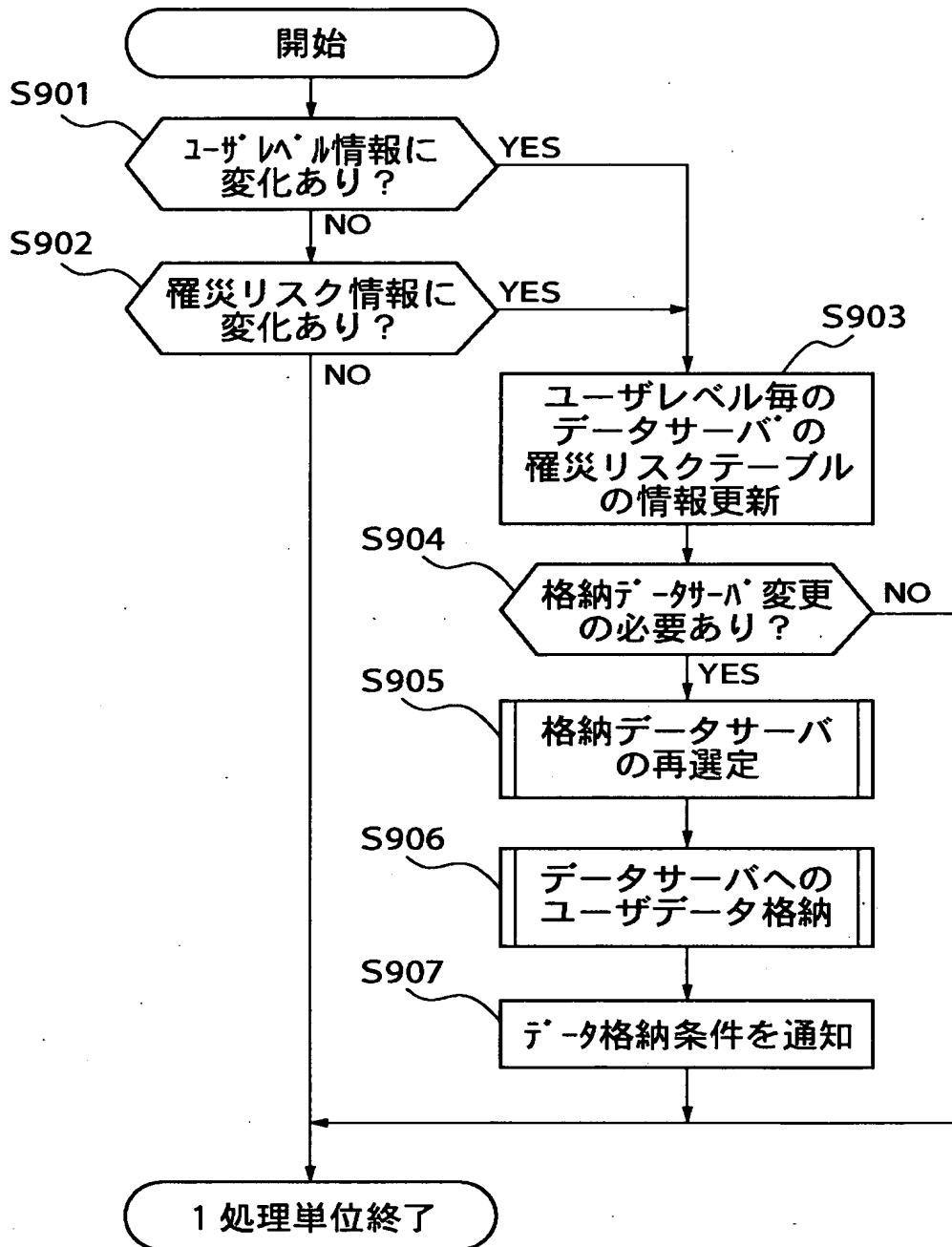
【図 9】



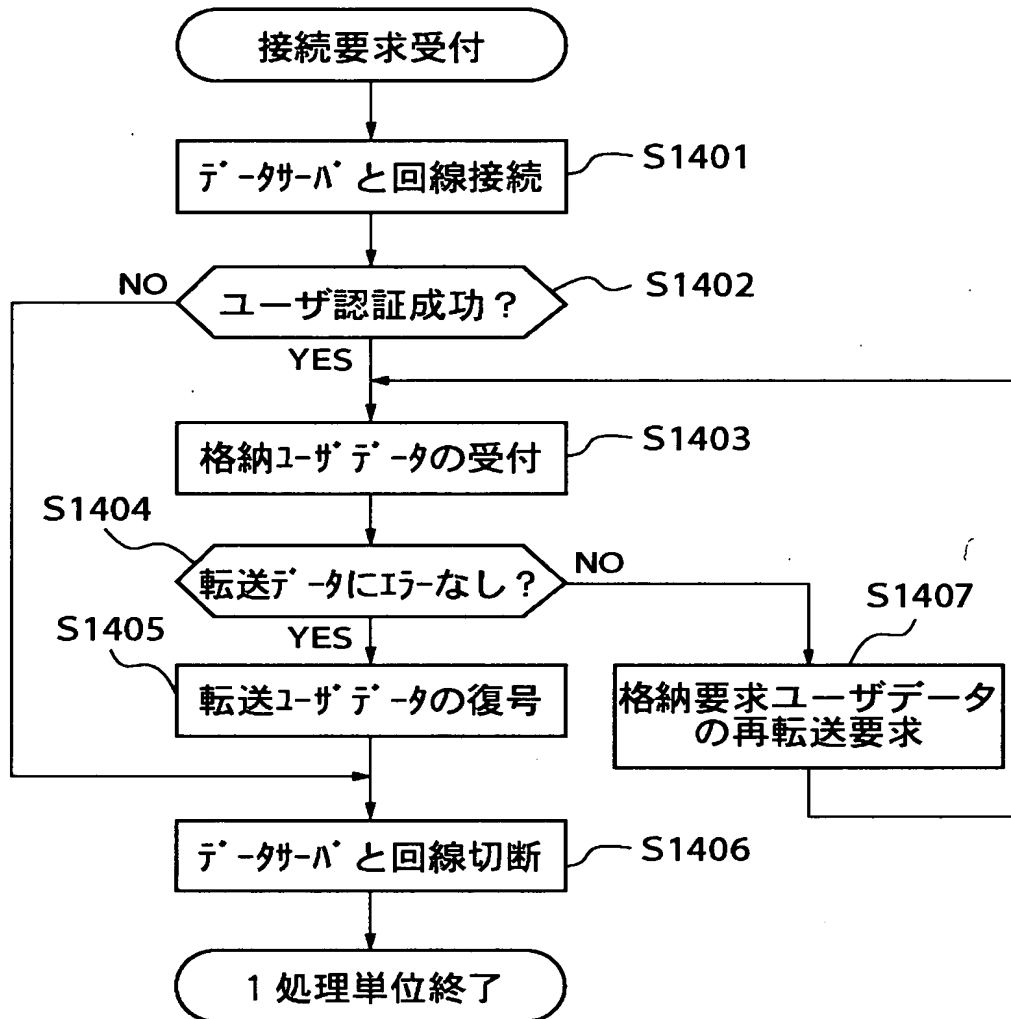
【図 1 0】



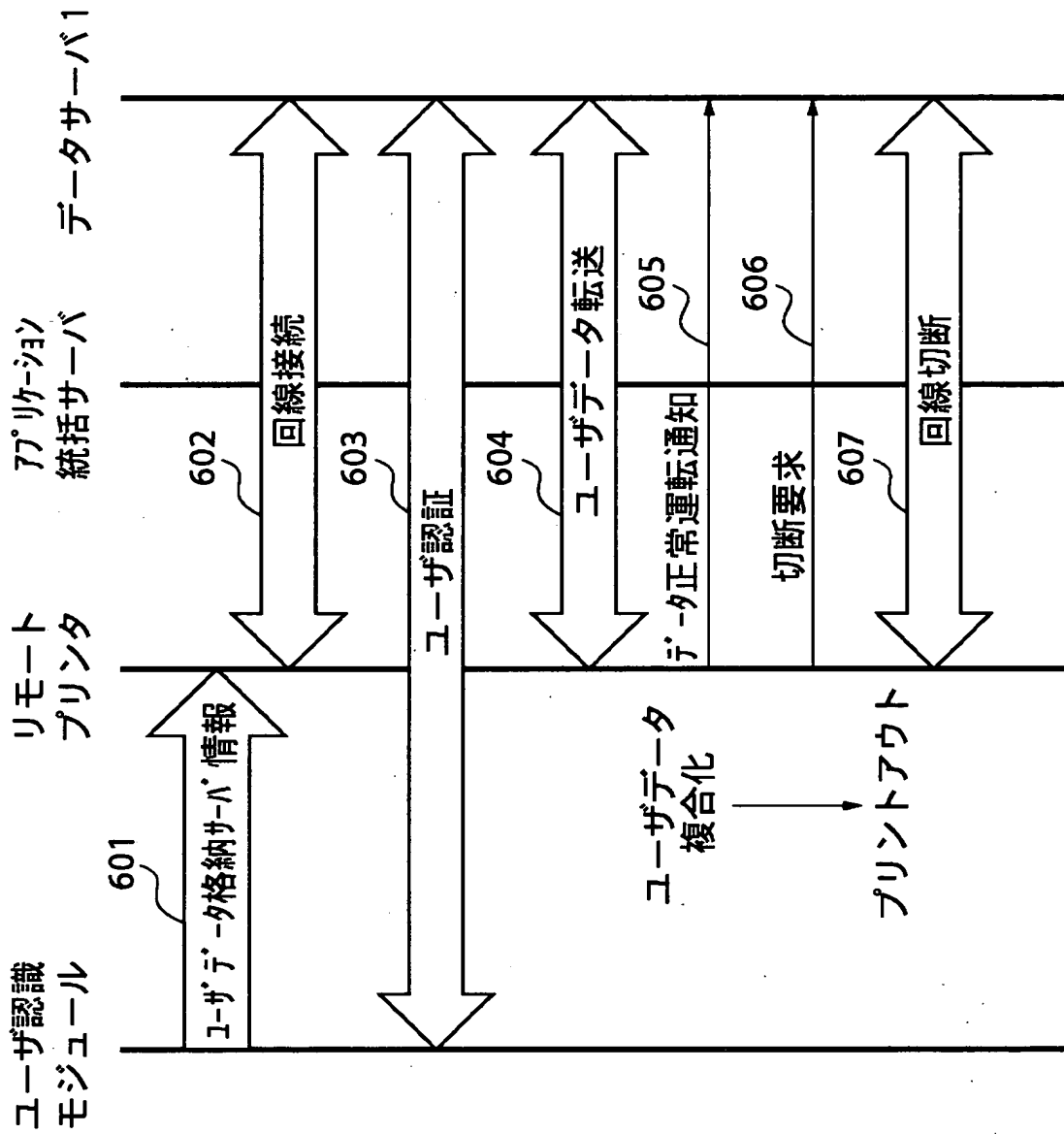
【図 1 1】



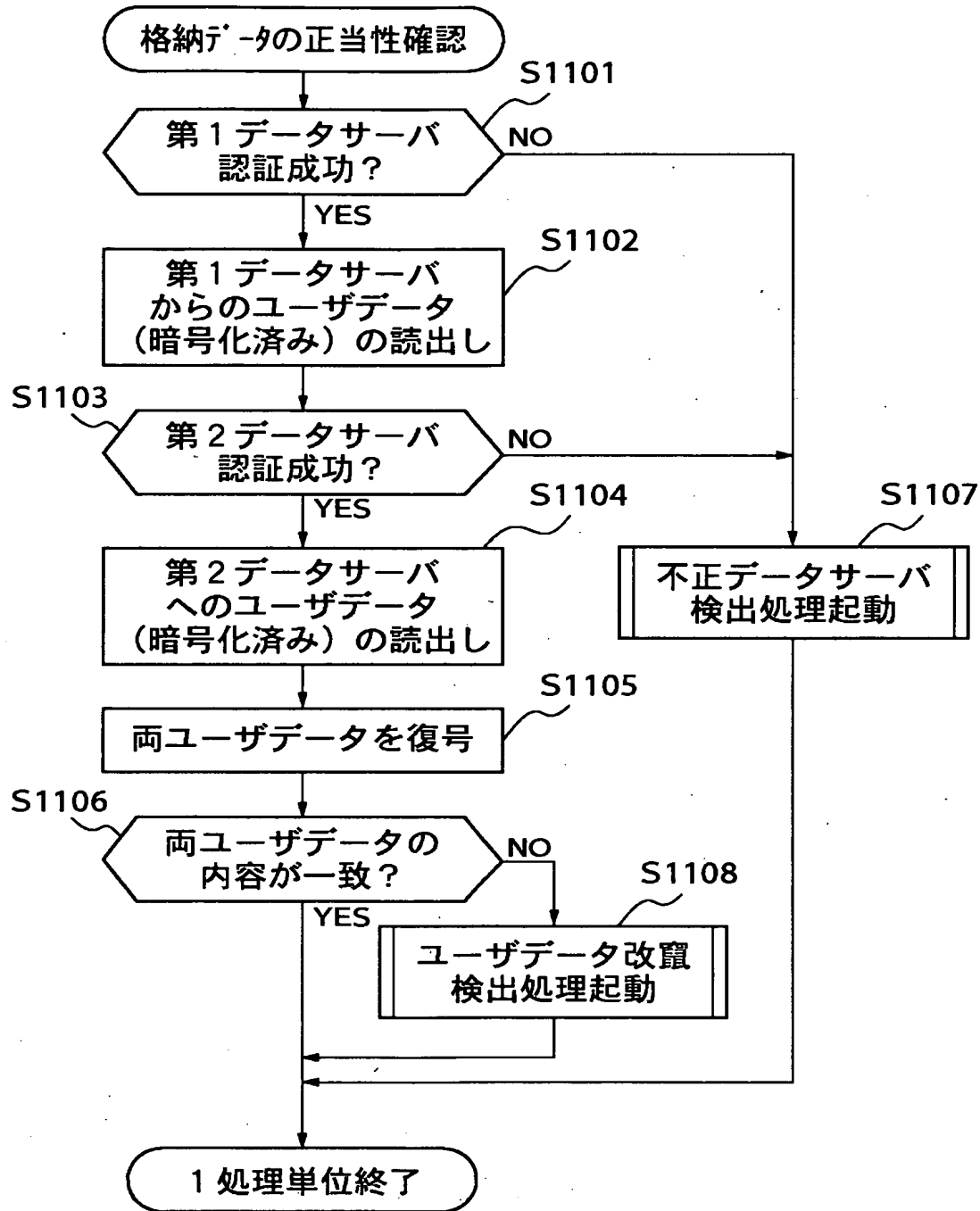
【図 1 2】



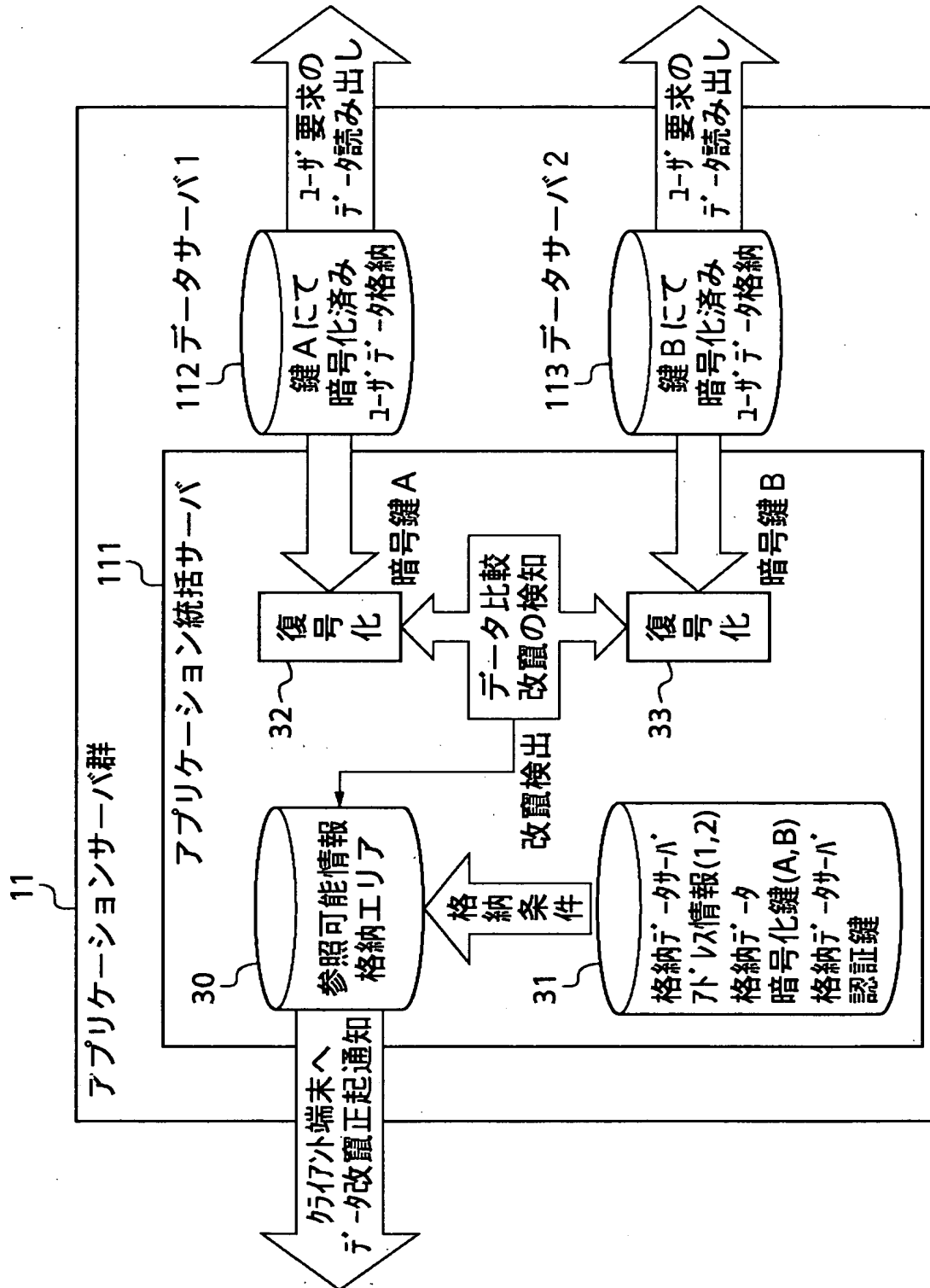
【図 13】



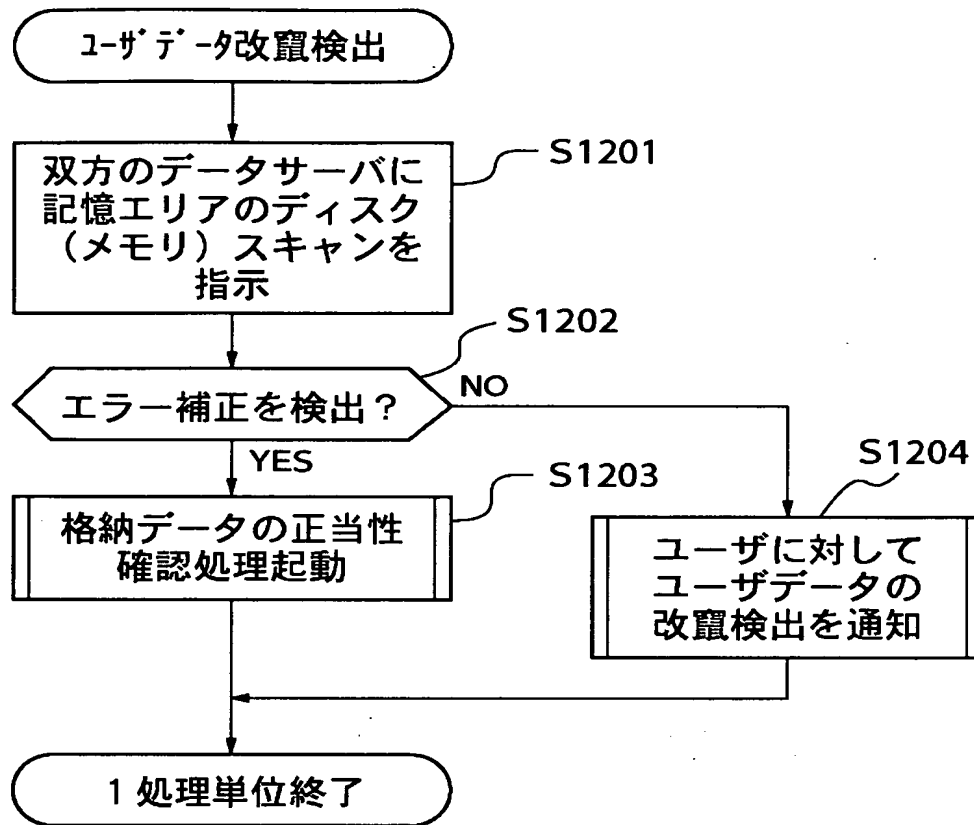
【図 1 4】



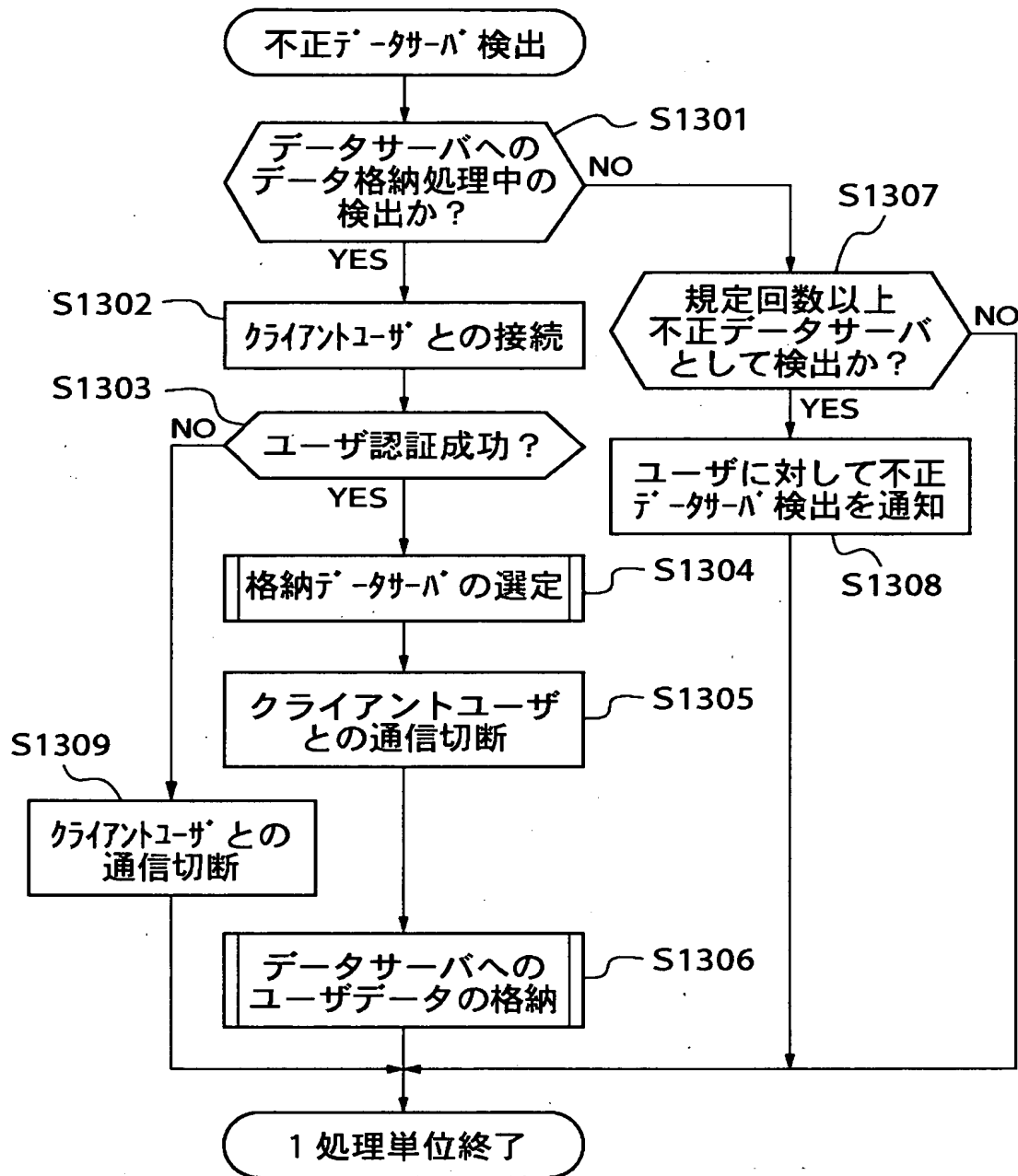
【図 15】



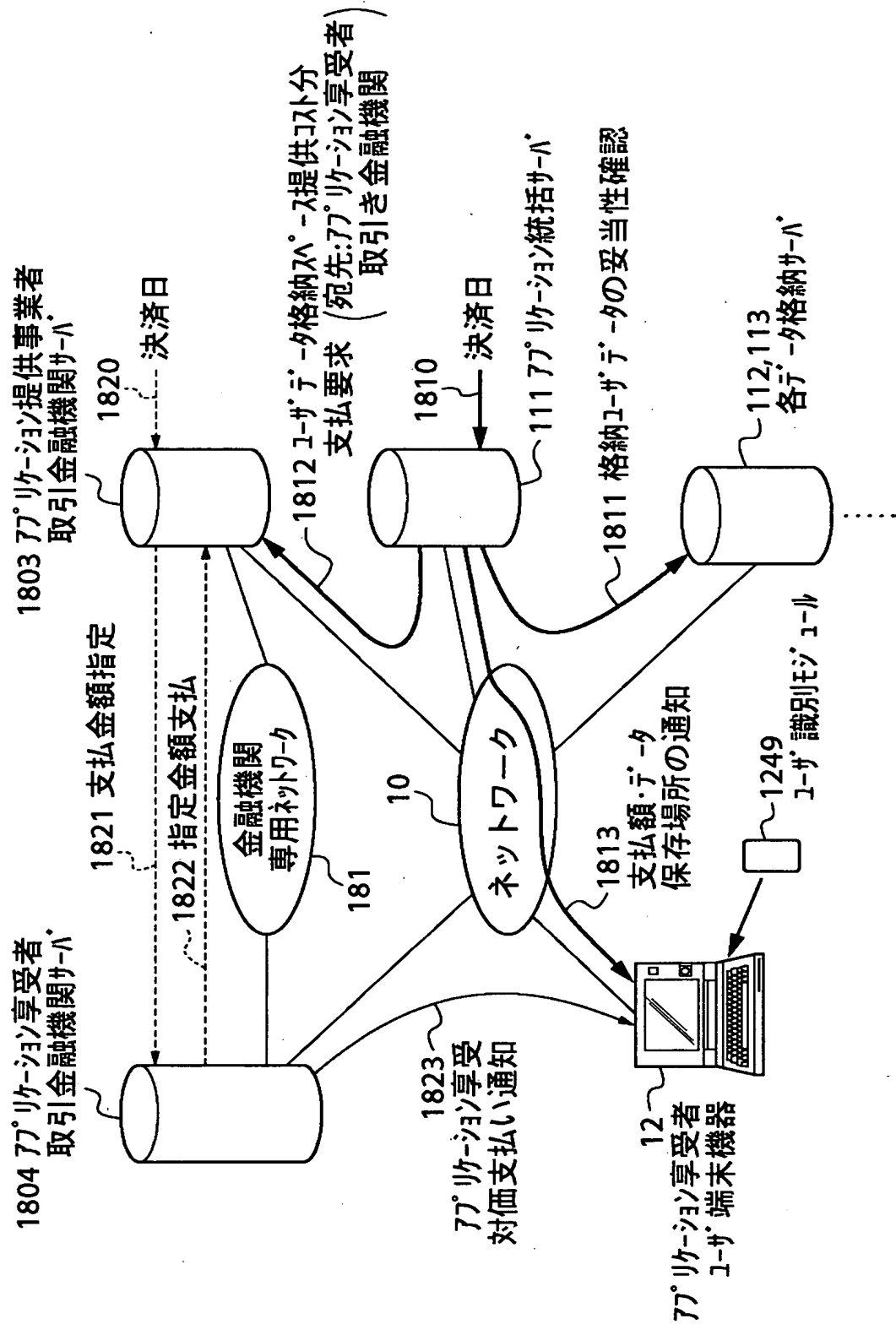
【図 1 6】



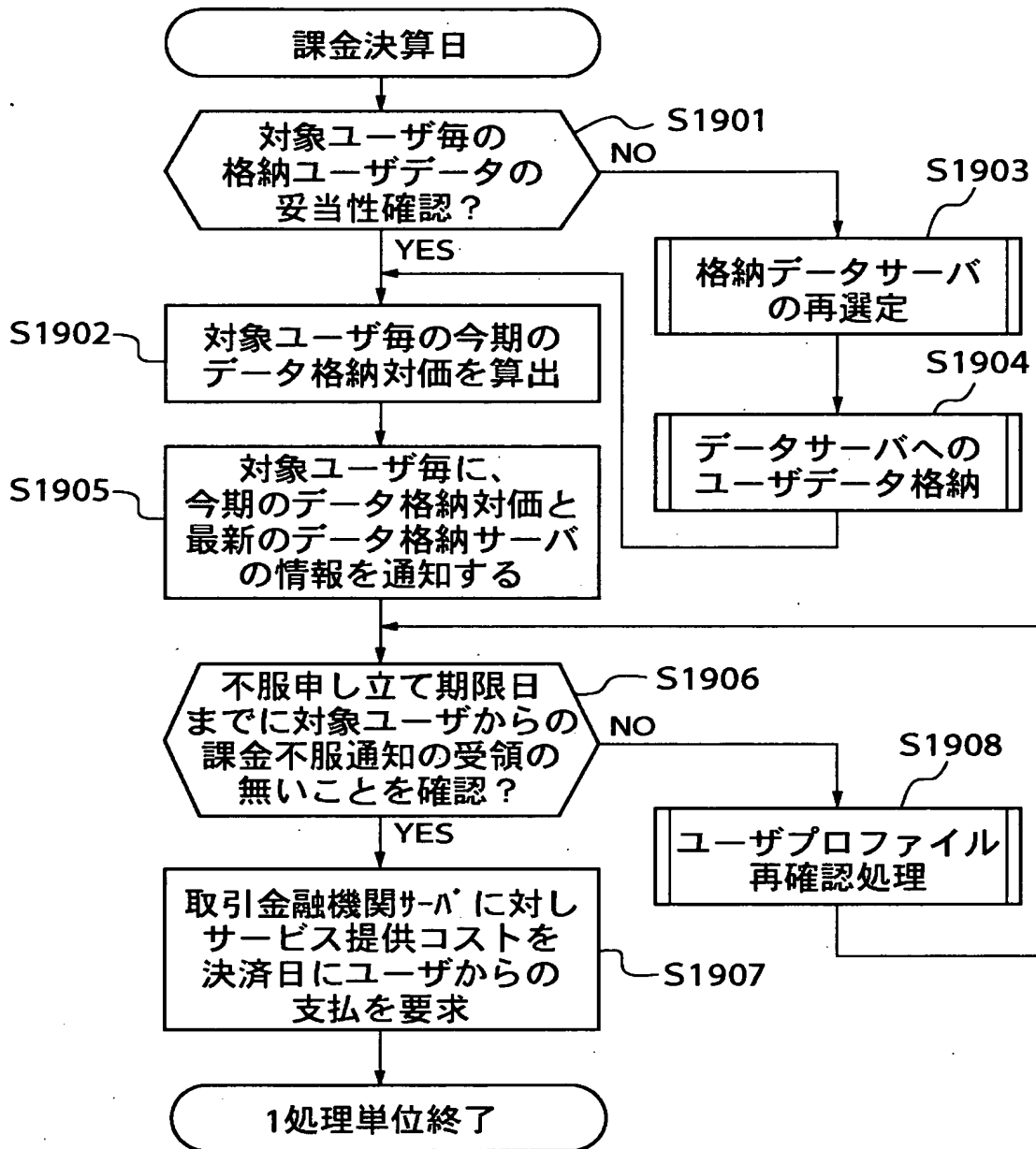
【図 1 7】



【図 18】



【図19】



【書類名】 要約書

【要約】

【課題】 利益効率を低下させることなく、公平なデータ保存サービスを提供できるようにする。

【解決手段】 ユーザのサービス加入条件のレベルに対応するサーバの中から、罹災リスクの最も低いサーバを選択し、その選択したサーバに対して保存要求に係るデータを格納する。

【選択図】 図 8

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都大田区下丸子3丁目30番2号
氏 名 キヤノン株式会社